STUDY OF CHAOS-BASED DIGITAL COMMUNICATIONS

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Philosophy in the Department of Electronic and Information Engineering of The Hong Kong Polytechnic University

by

Yip Ming, B.Eng

June 2000

ACKNOWLEDGEMENTS

The author wishes to express his appreciation to his supervisor Dr. Francis C.M. Lau for his invaluable advice, guidance and encouragement during the period of study. I also thank the academic staff members of the Department of Electronic and Information Engineering, especially Dr. S.F. Hau and Dr. C.K. Tse, for their fruitful discussions. In addition, I wish to thank Mr. Y.M. Wong for his technical support. Last but not least, it is my pleasure to acknowledge the inspiring discussions with my fellow colleagues.

ABSTRACT

Chaos communications have received much attention recently because chaotic signals can provide an alternate means to spread the spectrum of signals in digital communications. As in other spread spectrum techniques such as direct sequence code division multiple access and frequency hopping, chaos communications can provide secure communications with low probability of detection as well as mitigation of multipath fading effect.

In conventional communication systems, the allocated spectrum is shared by a number of users. Multiple access techniques such as frequency division multiple access, time division multiple access and code division multiple access are commonly used. Since chaos communications spreads the spectrum of the data signal over a much larger bandwidth, multiple access becomes an essential feature for practical implementation of the system. Furthermore, it is imperative that more users are included in the same bandwidth without causing excessive interference to one another.

In this thesis, an in-depth study of chaos-based digital communications using chaos shifting keying (CSK) and differential chaos shift keying has been performed. Multiple access schemes have been proposed in both systems. To verify the feasibility of the schemes, a simple 1-dimensional iterative map has been used to generate the chaotic signals for the users, and computer simulations are carried out to find the bit error probabilities (BEPs). For this simple map, it is found that numerical BEPs can be derived for different number of users. Simulations are performed and the results agree well with the numerical BEPs.

In practice, noise appears in any communications channel. To investigate the performance of the multiple access CSK scheme under such an environment, an additive white Gaussian noise source is added to the transmitted signal at the receiving end. It is found that a similar numerical BEP can again be derived. Simulations are performed and the simulated BEPs are consistent with the numerical ones. Although the results are not as good as conventional direct sequence spread spectrum systems using Gold codes as the spreading codes, chaos communications can provide a comparatively more secure means of communications.

LIST OF ABBREVIATIONS

APLL	analog phase-locked-loop
ASK	amplitude shift keying
AWGN	additive white Gaussian noise
BEP	bit error probability
BPSK	binary phase-shift-keying
CDMA	code division multiple access
COOK	chaotic on-off-keying
CSK	chaos shift keying
DCSK	differential chaos shift keying
DS-SS	direct sequence spread spectrum
FDMA	frequency division multiple access
FH-SS	frequency hopping spread spectrum
FM	frequency modulation
FM-DCSK	frequency modulated differential chaos shift keying
FSK	frequency shift keying
GPS	Global Positioning System
MA-DCSK	multiple access differential chaos shift keying
pdf	probability density function
psd	power spectral density
PSK	phase shift keying
SNR	signal-to-noise ratio
TDMA	time division multiple access

TH-SS	time hopping spread spectrum
WLAN	wireless local area network

LIST OF SYMBOLS

Φ	normal random sequence with elements $\{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, \ldots\}$
α	half of the spreading factor in a MA-DCSK system
β	spreading factor in a coherent CSK system
$\gamma_x(k,l,L)$	partial discrete auto-correlation function of the chaotic series $\{x_n\}$ with length L and a relative time shift of $k-l$ units
$\gamma_{xx'}(k,l,L)$	partial discrete cross-correlation function of the chaotic series $\{x_n\}$ and $\{x'_n\}$ with length L and a relative time shift of $k-l$ units
$\overline{\gamma_x(\kappa,\kappa,\beta)}$	mean-squared values of the chaotic sequence samples of length β
$\gamma_{x\phi}(k,l,L)$	partial discrete cross-correlation function of the chaotic series $\{x_n\}$ and the normal random sequence $\{\phi_n\}$ with length L and a relative time shift of $k-l$ units
$\theta_x(k,l)$	discrete auto-correlation function of the series $\{x_n\}$, with a relative time shift of $k-l$ units
$\theta_{xx'}(k,l)$	discrete cross-correlation function of the series $\{x_n\}$ and $\{x'_n\}$, with a relative time shift of $k-l$ units
$\sigma^2_{E_{-1}}$	variance of the received bit energy $\overline{E}_{-1}$
$\sigma^2_{E_{+1}}$	variance of the received bit energy $\overline{E}_{+1}$
$\sigma^2_{n'}$	variance of ξ_k
ξ_k	amplitude of the kth rectangular pulse of $n'(t)$

$c_{-1}(t)$	chaotic signal to be sent if data "–1" transmitted
$c_{+1}(t)$	chaotic signal to be sent if data "+1" transmitted
$\mathrm{Corr}_{-1}(mT_b)$	output of the correlator$_{-1}$ at the end of the mth symbol period
$\mathrm{Corr}_{+1}(mT_b)$	output of the correlator$_{+1}$ at the end of the mth symbol period
d_m	mth transmitted data
$d_{i,m}$	mth transmitted data for user i
$\mathrm{data}^m(t)$	data sample for the mth bit
$\mathrm{data}_i(t)$	data samples of user i
$\overline{E_{-1}}$	mean bit energy of chaotic sample function $c_{-1}(t)$
$\overline{E_{+1}}$	mean bit energy of chaotic sample function $c_{+1}(t)$
$\overline{E_b}$	average bit energy
E_{br}	received bit energy
$\overline{E_{bt}}$	average transmitted bit energy of the system
$\overline{E_{\mathrm{sep}}}$	separation between the two mean bit energies $\overline{E_{-1}}$ and $\overline{E_{+1}}$
$g(x)$	cubic map used to generate the chaotic signal x
G_u and G_v	Gold sequences belonging to the same set of Gold codes with a period of M
$n(t)$	additive white Gaussian noise
$n'(t)$	equivalent noise signal in a coherent CSK system
N	number of users
N_0	noise power spectral density
$p(t)$	received signal

$p'(t)$	received signal in the equivalent model of a CSK digital communications system
P^-	probability of a "−1" being transmitted
P^+	probability of a "+1" being transmitted
$r(t)$	rectangular pulse of unit amplitude and width T_c
$\mathrm{ref}^m(t)$	reference sample for the mth bit
$\mathrm{ref}_i(t)$	reference samples of user i
$s(t)$	transmitted signal
$s_i(t)$	transmitted waveform for user i
$s_u(t)$	transmitted waveform for user u
$s_v(t)$	transmitted waveform for user v
$S_n(f)$	two sided power spectral density of $n(t)$
T_b	bit duration
T_c	chip duration
T_s	acquisition time of the coherent CSK demodulator
$v^m(t)$	transmitted waveform for the mth bit
$v_i^m(t)$	transmitted waveform for the mth bit of user i
$\{x_n\}$	chaotic series
$\{x'_n\}$	chaotic series
$\{x_{\pm i,n}\}$	pair of chaos series for user i
$y_{i,m,f}(t)$	reference sample at the mth half-bit slot of the fth data frame for the ith user

$z(mT_b)$	the mth-sampled output of the adder of the coherent CSK demodulator
$z_{noise}(mT_b)$	output of the correlator at the end of the mth period under noisy environment
$z_i(mT_b)$	the mth-sample input to the threshold detector of user i
$z_{-1}(mT_b)$	the mth-sample input to the threshold detector given a "–1" has been transmitted
$z_{+1}(mT_b)$	the mth-sample input to the threshold detector given a "+1" has been transmitted
$\overline{z_{-1}(mT_b)}$	mean of $z_{-1}(mT_b)$
$\overline{z_{+1}(mT_b)}$	mean of $z_{+1}(mT_b)$
$z_i(f_i, m_i)$	output of the correlator of the ith user when the $[2(f_i-1)i+m_i]$th half-bit slot correlates with the $[2(f_i-1)i+i+m_i]$th half-bit slot

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

STATEMENT OF ORIGINALITY

The following contributions reported in this thesis are claimed to be original:

1. Statistical distribution of the partial discrete finite length auto- and cross-correlation functions of the cubic map. (Chapter 2)

   The mean-squared value of a chaotic sample of length L follows a normal distribution with mean 0.5 and variance dependent on L. For any two unequal chaotic samples, taken from different locations of the same chaotic series or from two different chaotic series, the correlation between them is normally distributed with zero mean and a variance dependent on the length L. The partial discrete cross-correlation function between the chaotic series and a normal random sequence, moreover, is normally distributed with zero mean, and a variance dependent on the length L as well as the variance of the random sequence. In general, the longer the length L, the smaller the variances will be in all cases.

2. A systematic approach to evaluate the bit error probability of a coherent CSK system in a noisy multi-user environment has been developed. (Chapter 4)

   The statistical properties of the correlator outputs of a coherent CSK receiver have been derived. Based on these properties, the numerical bit error probabilities are calculated. Simulations are also performed to verify the numerical values.

3. A simple multiple access scheme for use with differential chaos shift keying has been proposed. (Chapter 5)

   The delays between the reference samples and data samples are different for different users such that low auto- and cross-correlation values are achieved between samples from different users. Corresponding noncoherent receivers are also designed to decode the signals. The numerical bit error probabilities of the system are derived and compared with the simulation results. The proposed scheme achieves unbiased error probabilities for all users and the error performance degrades as the number of users increases. However, the spreading factor can be increased to improve performance.

LIST OF PUBLICATIONS

1. F.C.M. Lau, M.M. Yip, and C.K. Tse, "An approach to calculating the bit error probability of a coherent chaos-shift-keying digital communication system under a noisy multi-user environment", submitted to IEEE Trans. on Circuits and Systems I—Fundamental Theory and Applications.
2. F.C.M. Lau, M.M. Yip, C.K. Tse and S.F. Hau, "A Multiple Access Technique for Differential Chaos Shift Keying," submitted to IEEE Trans. on Circuits and Systems I—Fundamental Theory and Applications.
3. F.C.M. Lau, M.M. Yip, C.K. Tse and S.F. Hau, "A Multiple Access Technique for Differential Chaos Shift Keying," IEEE International Symposium on Circuits and Systems 2001, May 2001, Sydney, Australia. (Paper accepted)

CHAPTER 1

INTRODUCTION

1.1 Spread Spectrum Communications

1.1.1 What is Spread Spectrum?

Spread spectrum communications emerged from research efforts during the Second World War to provide a secure means of communications in adverse conditions. Most of the work remained classified until the 1970s. Nowadays spread spectrum becomes one of the most popular technologies used in wireless communications. To be categorized as a spread-spectrum system, the modulation/demodulation must have the following characteristics [Pete 95]:

1. The transmitted signal must occupy a bandwidth larger than (normally much larger than) the information bit rate and the occupied bandwidth is approximately independent of the bit rate.
2. Demodulation must be achieved, in part, by correlating the received signal with a replica of the signal used in the transmitter to spread the information signal.

1.1.2 Advantages

When the signal power is spread over a larger bandwidth, the average power spectral density (psd) becomes lowered. As a consequence, the psd may not be much higher than the background noise. Without prior knowledge of the transmitted signal or

sophisticated equipment, it is not easy to detect the presence of the signal. Even if an unintended user detects the presence of the signal, without the appropriate spreading code, it is very difficult for him to decode the data.

In a narrowband system, the whole communications link breaks down if someone jams the signal with a single tone lying within the signal bandwidth. On the other hand, if the signal is spread before transmission, the effect of the single jamming tone can be reduced substantially after the de-spreading process in the receiver. That is why spread spectrum communications have been used in the military for years.

1.1.3 Techniques

There are two main streams of spread spectrum techniques — direct sequence and frequency hopping.

In a direct sequence spread spectrum (DS-SS) communications system, each data symbol$\in \{-1,+1\}$ is multiplied by a sequence of binary codes$\in \{-1,+1\}$ (spreading code). Since the spreading code is generated at a much higher rate than the data, the resultant signal occupies a much larger bandwidth. On the receiving side, the incoming signal is multiplied by the same spreading code to de-spread the signal. If the channel does not cause much distortion to the signal, and the interference and noise levels are not so high, the exact data sequence can be recovered. Figure 1-1 depicts the data symbols as well as the waveforms after the spreading and de-spreading processes at the transmitter and receiver respectively. The spreading factor is defined as the ratio of data symbol duration to spreading code chip duration. Note that ideal timing synchronization has been assumed and no carrier has been used for simplicity. Figure 1-2 shows the block diagram of a simplified binary phase-shift-keying (BPSK) DS-SS transceiver.

In DS-SS communications, the spread signal has to transmit in a contiguous frequency band. In frequency hopping spread spectrum (FH-SS) communications, however, such requirement is not needed. It is because in FH-SS, the bandwidth of the data signal is not spread, but rather hops from one carrier to another. This is achieved by changing the carrier frequency from time to time. At the receiver, the local oscillator hops in a synchronized manner with the transmitter frequency pattern to down-convert the received signal. Without prior knowledge of the hopping pattern, it will be very difficult, if not impossible, to decode the information. Moreover, as the signal is now transmitted through a number of carriers, the channel degradation is averaged over all carriers. Figure 1-3 shows the block diagram of a FH-SS transceiver.

Other spread spectrum techniques include time hopping spread spectrum (TH-SS) and hybrid forms involving more than one spread spectrum techniques described above. More details can be found in [Dixo 94], [Pete 95], [Vite 95].

1.1.4 Applications

Besides military values, there are commercial applications of spread spectrum communications. For example, in mobile communications, the IS-95 standard [TIA 95] makes use of the DS-SS technique to spread the binary symbols in both uplink and downlink. Multiple access is then achieved by assigning different codes to different users.

Another application that utilises DS-SS is the Global Positioning System (GPS), also known as NAVSTAR [Clar 96], [Glob 86]. GPS makes use of 24 satellites in 12-hour orbits spaced uniformly around the earth whose positions are precisely known all the time. Two spread signals are transmitted by each satellite. If a user can decode the

signals from at least four different satellites which are in view simultaneously, he will be able to determine his position. Originally developed for military applications, GPS is now used in many civilian applications such as geodesic survey, navigation, fleet management, etc..

For FH-SS, the most commonly used applications include wireless local area network (WLAN) [Ieee 99] and the short range wireless communications protocol Bluetooth [Blue 00]. While both applications works in the unlicensed 2.4GHz band, up to 11 Mbps data rate is now available using FH-SS WLAN while Bluetooth supports up to 1Mbps transfer rate.

1.1.5 Multiple Access

In a multiple access spread spectrum communications system, all users are using the same spectrum to transmit their own signal at the same time. In DS-SS, users are differentiated by their codes (code division multiple access, CDMA). Ideally, orthogonal codes such as Hadamard codes [Proa 95] should be used to distinguish one user from another. However, the number of Hadamard codes available for a specific spreading factor is limited. For example, if a spreading factor of 64 is used, there are only 64 possible Hadamard codes available. If orthogonality is not necessary, spreading can be provided by other sequences such as maximal-length sequences (m-sequences) and Gold sequences [Pete 95]. Although the number of code sets is now larger, it is still limited. On the other hand, since the codes are no longer orthogonal, the cross-correlation between the codes will affect the bit error performances of the users.

In a practical communications system, it is not uncommon for the transmitted signal to travel through several different paths before arriving at the destination

(multipath propagation). Assume that the local code generator at the receiver is synchronized with the first signal arrived. Under such circumstance, if the time delay between different paths is comparable with the code period, the signals subsequently arrived will correlate with the delayed version of the local generator code, causing interference to the required signal. For a given spreading code and a given spreading factor, the adverse effect due to such undesired condition will depend on (a) the strength of the late-arrival signals, (b) the time delay of the signals, and (c) the part of the spreading code that is being de-spread. Using a spreading code with low full and partial auto-correlation functions, the effects of (b) and (c) can be reduced.

In FH-SS communications, if the number of users is comparable with the number of carriers and the hopping sequences of different users are not arranged in a proper way, there is a high probability that two or more users will transmit with the same carrier at the same time. In such case, all collided signals will be corrupted. Even if all the hopping sequences of the users are synchronized, the number of users is still limited by the number of available carriers. If all the carriers are occupied, the carriers of any additional user are bound to collide with those of other users.

1.2 Chaos Communications

1.2.1 What is Chaos?

Chaos [Alli 96], [Deva 92], [Mull 93] is a non-periodic, bounded signal derived from a set of differential or difference equations. It looks like random but is in fact deterministic. Because of the random-like feature, chaotic signals occupy a wide bandwidth. Another characteristic of chaos is its sensitive dependence on initial conditions. A slight change in the initial condition will alter the path of chaos

substantially as time moves on. Hence, in theory, an infinite number of chaotic signals can be generated from the same set of differential or difference equations by using different initial conditions.

1.2.2 Advantages

Chaotic signals, with their inherent wideband characteristic, can be applied to transmit narrowband signals. The resultant signal, having a higher bandwidth and lower psd, will not be easily detected. Moreover, degradation due to multipath fading can be mitigated and a large number of spreading waveforms can be produced easily by changing the initial conditions. Several analog and digital modulation schemes based on chaos have been proposed recently and they are introduced in the following sections.

1.2.3 Analog Modulation Based on Chaos

There are two main techniques to spread analog information by chaotic signals — chaotic masking [Koca 92] and chaotic modulation [Itoh 95]. In chaotic masking, the analog signal is spread by adding it to the output of a chaotic system. The resultant signal is modulated and transmitted. At the receiving end, the analog information is extracted from the combined signal. In chaotic modulation, the analog information is injected into a chaotic circuit. Such action changes the dynamics of the chaotic circuit. At the receiver, the change in dynamics of the incoming chaotic signal is tracked and the analog signal is recovered.

1.2.4 Digital Modulation Based on Chaos

Several chaotic modulation schemes [Jako 98], [Kenn 98a], [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a], [Kolu 97a], [Kolu 97b], [Kolu 98] have been proposed over the past few years. They mapped binary symbols to nonperiodic chaotic basis functions. Among the chaotic modulation techniques, chaos shift keying (CSK) [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a] maps different symbols to different chaotic attractors, which are produced by a dynamical system for different values of a bifurcation parameter or by completely different dynamical systems. A coherent correlation CSK receiver is then required at the receiving end to decode the signals. Noncoherent detection is also possible provided the signals generated by the different attractors have different attributes, such as mean of the absolute value, variance and standard deviation. However, in this case, the optimal decision level of the threshold detector will depend on the signal-to-noise ratio.

In chaotic on-off-keying (COOK) [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a], the chaotic signal is turned on/off by the binary data to be transmitted. In other words, the transmission of the chaotic signal is enabled when the transmitted bit is "–1", and the signal is disabled for bit "+1". Maximum distance between the elements of the binary symbols can then be achieved for a given average bit energy. At the receiver, the bit energy carried by the signal is first estimated and then compared against a threshold. Depending on whether the bit energy is larger or less than the threshold, the bit will be decoded as "–1" or "+1" respectively. A noncoherent detector can be used in this case. Unfortunately, the decision level of the threshold detector still depends on the signal-to-noise ratio.

To overcome the threshold level shift problem, differential CSK (DCSK) is proposed [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a]. In DCSK, every transmitted symbol is represented by two chaotic signal samples. The first one serves as the reference (reference sample) while the second one carries the data (data sample). If a "+1" is to be transmitted, the data sample will be identical to the reference sample, and if a "−1" is to be transmitted, an inverted version of the reference sample will be used as the data sample. The advantage of DCSK over CSK and COOK is that the threshold level is always set at zero and is independent of the noise effect. In [Kis 98b], it has been shown that by increasing the length of the chaotic sample or the bandwidth of the carrier, the variance of the estimation can be reduced, resulting a lower bit error probability (BEP).

Because of the non-periodic nature of chaos, the bit energy of the transmitted symbol using CSK, COOK and DCSK varies from one bit to another. To produce a wideband chaotic signal with constant power, a chaotic signal, generated by an appropriately designed analog phase-locked-loop (APLL) is fed to a frequency modulator (FM modulator). It has been shown in [Kenn 99] that the output has a bandlimited spectrum with uniform power spectral density. It can then be further combined with other modulation techniques such as DCSK to form frequency modulated DCSK (FM-DCSK) [Kenn 98b], [Kenn 99], [Kis 98a], [Kolu 97b], [Kolu 98].

The noise performances of DCSK and FM-DCSK have been shown to improve by cleaning the noisy sample functions at the receiving end [Jako 98]. In [Kenn 98a], [Kolu 97a], a multilevel DCSK has been proposed to improve the spectral efficiency of DCSK.

The aforementioned digital modulation schemes based on chaos, namely CSK, COOK, DCSK and FM-DCSK, will be further discussed in Chapter 3. However, there are two points to note here. First, the chaotic signals used to transmit the binary symbols are analog in nature which can be generated by continuous-time or discrete-time systems. Second, although the system transmits a signal with a much larger bandwidth than the information bit rate and the occupied bandwidth is approximately independent of the bit rate, strictly speaking, it may not be classified as a spread spectrum communications system. It is because if noncoherent detection can be applied to recover the data, it will not be necessary to correlate the received signal with a replica of the chaotic signal used in the transmitter. In the next section, chaos-based spread spectrum communications systems are briefly discussed.

1.2.5 Spread Spectrum Communications using Chaos

In Section 1.1, it has been mentioned that *m*-sequences and Gold sequences can be applied to spread the data symbols in a conventional DS-SS communications system. The spreading sequences, on the other hand, can be designed based on chaos. One simply way to obtain spreading codes based on chaos is to quantize the output of a discrete-time chaotic signal and convert it into binary codes. In [Mazz 97] and [Mazz 98], a thorough analysis is presented on the achievable performance of a classical DS-SS communications system when the spreading sequences are generated by quantizing and periodically repeating a slice of a chaotic time-series. It has been found that chaos-based sequences do not behave worse than *m*-sequences and Gold sequences. Another approach to generate spreading codes based on two chaotic maps can be found in [Heid

94]. In [Sett 99], the issues of phase acquisition and tracking needed for synchronization between the spreading and de-spreading sequences have been investigated.

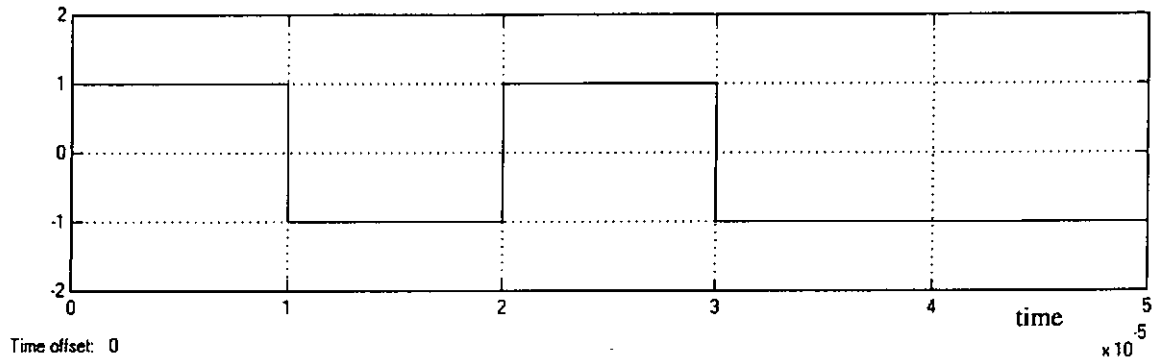
1.2.6 Multiple Access

Since chaos communications spread the spectrum of the data signal over a much larger bandwidth, multiple access becomes an essential feature for practical implementation of the system. Furthermore, it is imperative that more users are included in the same bandwidth without causing excessive interference to one another. Some basic work has been reported on multiple access in chaos-based communications such as multiplexing chaotic signals [Carr 99] and exploiting chaotic functions for generating spreading codes under the conventional code division multiple access (CDMA) scheme [Yang 97]. However, very little work has been reported so far on direct implementation of a multiple access scheme in a chaos-based digital communications system such as one that is based on CSK or DCSK.

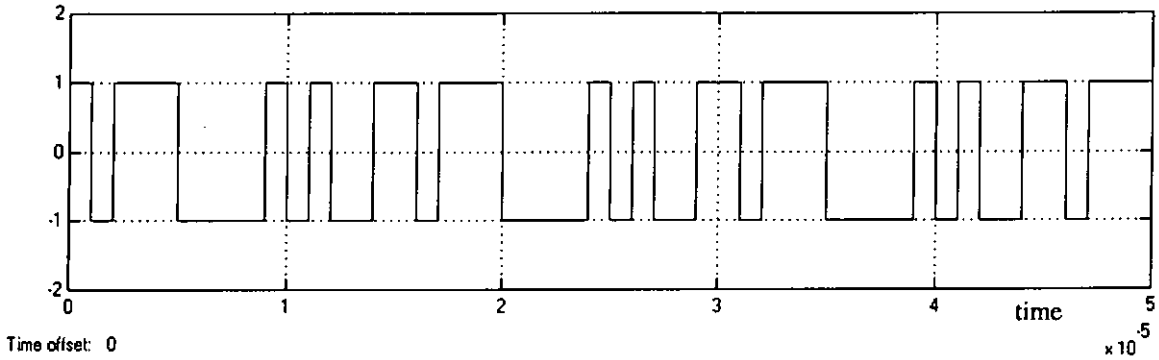
1.3 Motivation and Organization of the Thesis

In this thesis, we investigate two chaos-based digital modulation schemes, CSK and DCSK, under a multi-user environment in detail. Multiple access in CSK is studied under coherent detection while noncoherent detection is assumed in DCSK. In Chapter 2, we will briefly introduce the characteristics of chaotic signals in general. Properties of several types of chaotic signals will be compared. The features of the chaotic signal used in this thesis, moreover, will also be shown in greater detail. In Chapter 3, existing chaos-based digital modulation schemes will be reviewed. The advantages and disadvantages of the schemes will also be compared. Some typical results are also

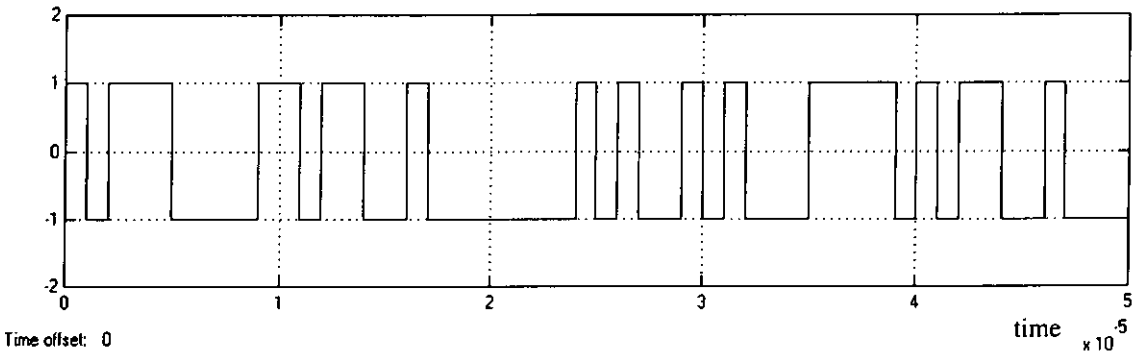
shown. Chapter 4 presents an in-depth study of CSK. The performance of a single-user system will be studied first. Under a multi-user environment, the properties of the received signals will be further analyzed. Bit error performances of the systems under clean and noisy channel conditions will be investigated. Two different spreading ratios are tested and the simulation results are compared with the numerical solutions. Then the results are compared with those of a conventional spread spectrum communications systems using Gold code as the spreading code. In Chapter 5, a novel multiple access technique based on differential CSK (DCSK) is proposed. Simulation results as well as numerical solutions are again presented. A critical review of the thesis will be given in Chapter 6 and conclusions are drawn in Chapter 7.



(a) transmitted data symbols (bit duration $T_b = 10^{-4}$ s)

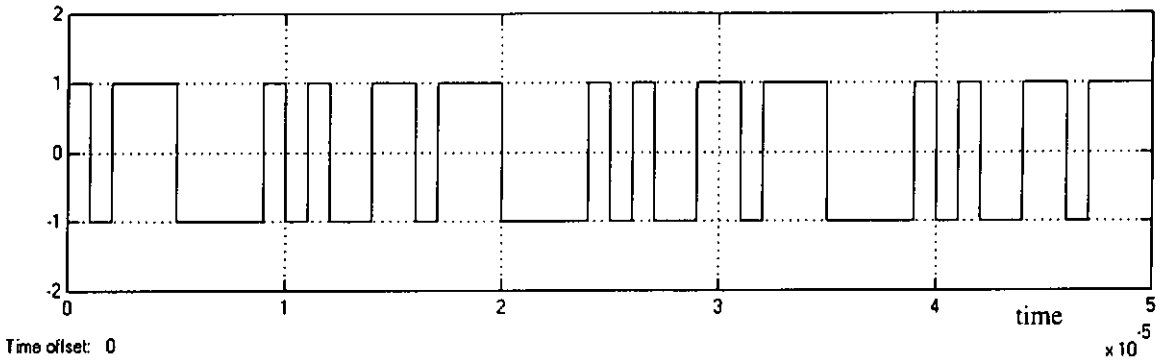


(b) spreading code (chip duration $T_c = 10^{-5}$ s)

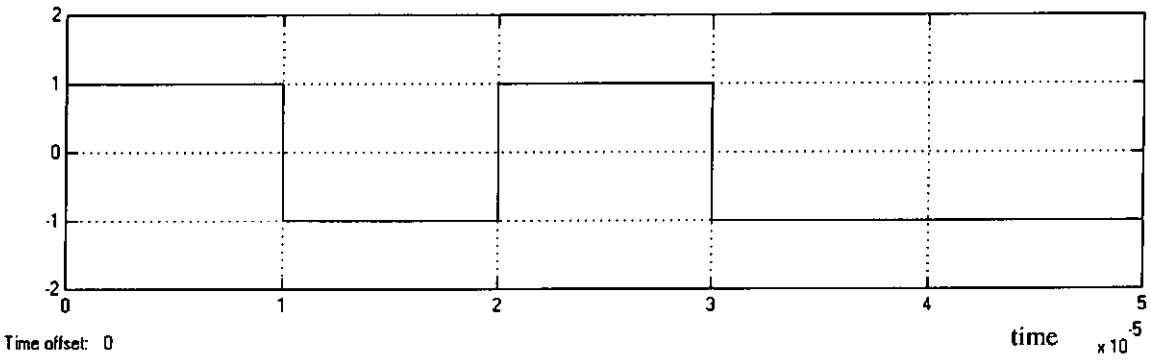


(c) transmitted waveform after spreading

Figure 1-1 Waveforms in a direct sequence spread spectrum communications system (spreading factor = 10)



(d) de-spreading code



(e) recovered waveform after de-spreading

Figure 1-1 Waveforms in a direct sequence spread spectrum communications system (spreading factor = 10)

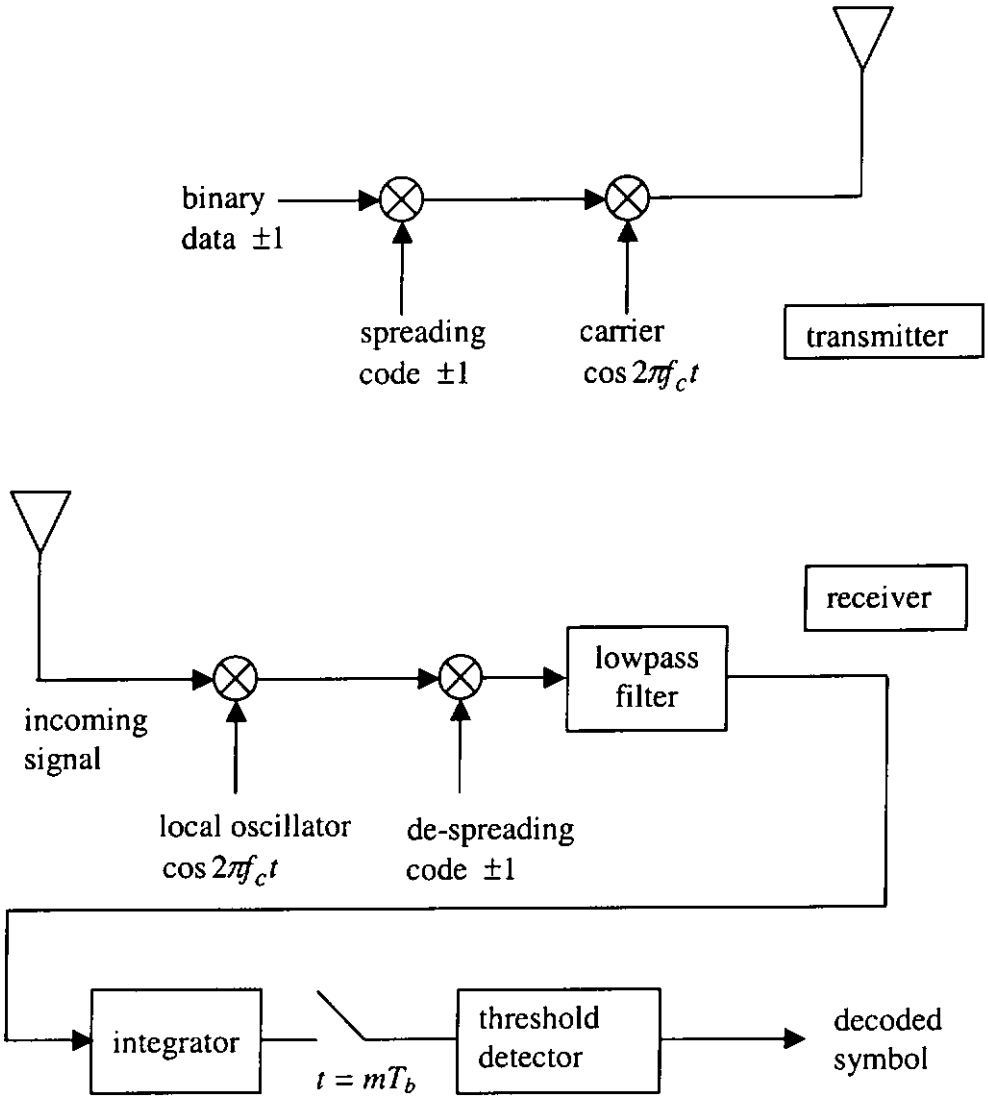


Figure 1-2 Block diagram of a simplified binary phase-shift-keying DS-SS transceiver

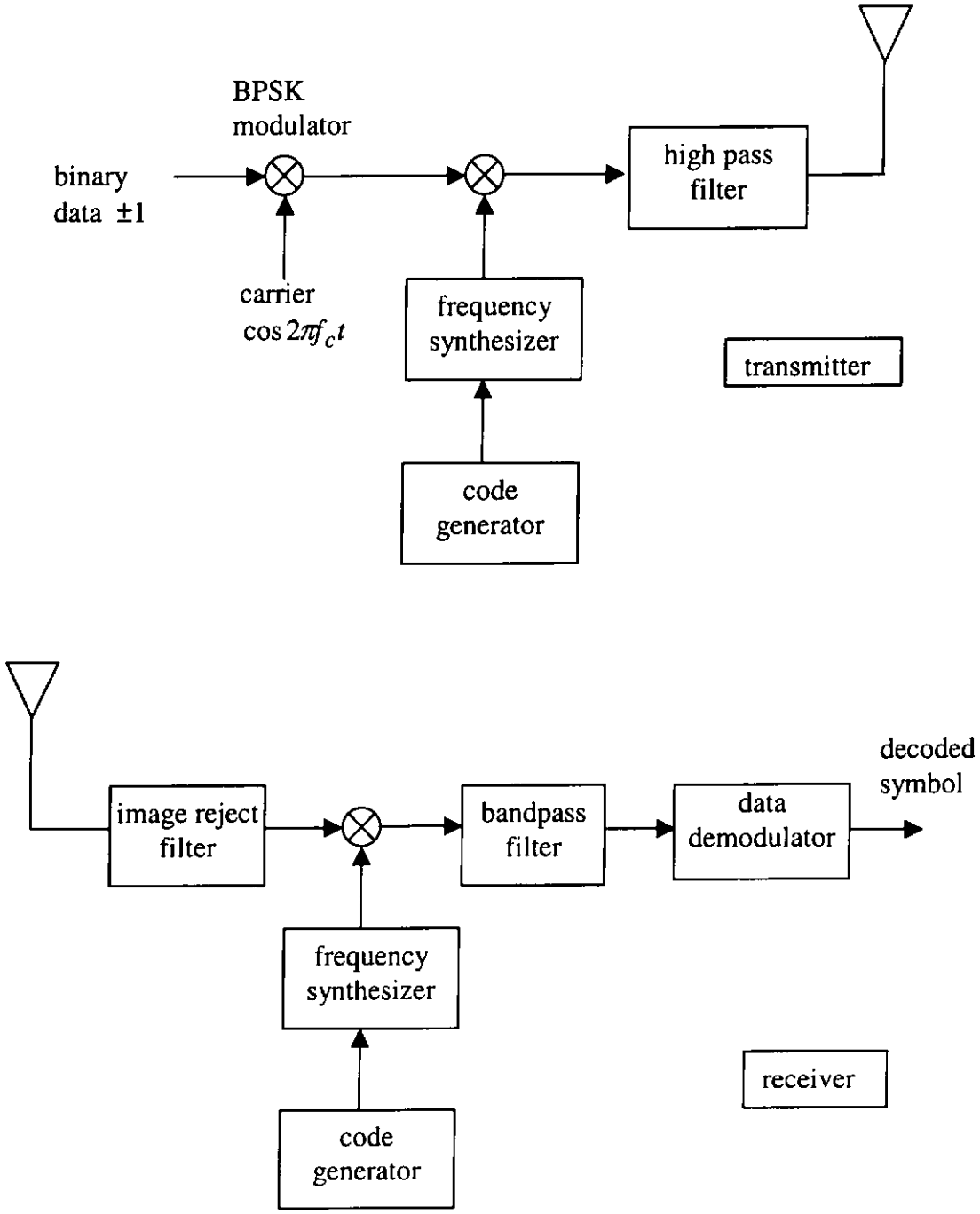


Figure 1-3 Block diagram of a frequency hopping spread spectrum transceiver

CHAPTER 2

CHAOS

Chaos is characterized by its sensitive dependence on initial conditions, deterministic and yet random-like behaviour. It can be generated by continuous-time and discrete-time systems. In this chapter, we will study some typical properties of chaos in detail. The criteria for choosing a chaotic signal in chaos-based digital communications are also presented. Several simple maps are introduced. Among them, one has been selected by the author for further analysis. The characteristics of this chaotic signal, especially its partial discrete auto-correlation and cross-correlation functions, have been investigated.

2.1 Dynamical System

A dynamical system is comprised of "a set of possible states, together with a rule that determines the present state in terms of the past states" [Alli 96]. For example, if the population of a country increases by 10% every year and the population now is denoted by x_n, the population next year is given by

$$x_{n+1} = g(x_n) = 1.1x_n. \tag{2-1}$$

Here the variable n stands for time and x_n represents the population at time n.

2.1.1 Types of Dynamical Systems

There are mainly two types of dynamical systems — discrete-time and continuous-time. In a discrete-time dynamical system, the rule is applied at discrete times. The system will take the current condition as the input and updates the condition by generating a new state as output, as in equation (2-1). When the update times get smaller and smaller, towards the limit zero, the governing rule becomes a set of differential equations. Then the system becomes a continuous-time dynamical system. For example, let

$$\dot{x} \equiv \frac{dx}{dt} = 1.1x \tag{2-2}$$

where x is a scalar function of t, and $\dot{x}$ denotes the instantaneous rate of change with respect to time. If x represents the size of population, the rate dx/dt at which the population grows will be proportional to the current population x of the system. (Note that in equation (2-1), the size of the new population is proportional to the previous population. Hence equations (2-1) and (2-2) represent different models.) Another example would be

$$x_{n+1} = 4x_n(1 - x_n) \tag{2-3}$$

and $\dot{x} = 4x(1 - x)$ (2-4)

where equation (2-3) is a logistic map and equation (2-4) is a logistic differential equation. Note that, again, they represent different models.

Using computer simulations, chaos can be generated much easily with discrete-time systems than continuous-time systems. Hence, in the following, we shall concentrate our discussions and analyses on discrete-time systems, also known as maps.

2.1.2 Types of Orbits

Consider the logistic map again

$$x_{n+1} = g(x_n) = 4x_n(1 - x_n) \text{ on } [0, +1]. \tag{2-5}$$

First x_n must lie between [0, +1] to ensure the solutions are in a bounded region of space. Then, depending on the initial conditions, the orbit, given by the set of points $\{x_0, x_1, x_2, ...\}$, generated by the map can be categorised into three main types.

2.1.2.1 Fixed Point

A point p is a fixed point of the map g if $g(p) = p$. In this particular map, it can be shown easily that the fixed points are at 0 and 3/4. If the initial condition equals to or if the orbit coincides with one of the fixed points, the system will remain at the fixed point forever.

2.1.2.2 Periodic Orbits

A point p is a periodic point of period k of the map g if k is the smallest positive integer such that $g^k(p) = p$. In other words, the system is oscillating between a number of points. The orbit with initial point p (which consists of k points) is called a periodic orbit of period k. For example, if the initial condition produces an orbit with a period of 2, we have $g^2(x_0) = x_0$. Solving for x_0, we obtain $x_0 = 0,\ 3/4,\ \frac{5 \pm \sqrt{5}}{8}$.

Since the points 0 and 3/4 are actually fixed points, only the values of $x_0 = \frac{5 \pm \sqrt{5}}{8}$ will generate orbits with period 2.

Note that certain initial conditions will have their orbits coincide with the periodic points eventually. Such orbits are called "eventually periodic orbits".

2.1.2.3 Chaotic Orbits

All other orbits besides the aforementioned ones are categorized as chaotic orbits. For example, an initial condition of 0.127 for the logistic map will create a chaotic orbit. The properties of chaos will be described in the following section.

2.2 Chaos and its Properties

2.2.1 Definition of Chaos

According to the Encyclopaedia Britannica the word "chaos" is derived from the Greek word "χαοζ". It originally meant "the infinite empty space which existed before all things". In the study of dynamical systems, chaos indicates "a third state in addition to the steady and the periodic states, provided the solutions are in a bounded region of space". This is the definition we shall adopt in this thesis. The fact that the solutions are bounded is a very important criterion because maps such as that in equation (2-1) will extend to infinity, no matter how small the initial condition is.

2.2.2 Properties of Chaos

In the following discussions, the logistic map (2-5) has been used to demonstrate some typical properties of chaos. Unless otherwise stated, the chaotic series $\{x_n\}$ is generated by the logistic map (2-5) with an initial condition of 0.127.

2.2.2.1 Aperiodic

Figure 2-1 plots the series $\{x_n\}$ as a function of n. Apparently, it is not in a steady state. Moreover, there is no observable period of the signal. In fact, no period is found even if the series is observed for a longer time.

2.2.2.2 Sensitive to Initial Conditions

Using two slightly different initial conditions 0.127 and 0.127001, the iterated function is plotted against n as in Figure 2-2. It can be shown that the two curves diverge after about 20 iterations. After that, little correlation can be observed between the two curves. In fact, no matter how close they begin, the two curves will diverge eventually. Hence the orbit of the map is sensitive to the initial conditions.

2.2.2.3 Discrete Auto-correlation Function

Chaotic signals de-correlate with themselves rapidly. Define the discrete auto-correlation function of the series $\{x_n\}$, with a relative time shift of $k - l$ units, as [Pete 95]

$$\theta_x(k,l) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=-\zeta}^{N-1-\zeta} x_{k+n} x_{l+n} \tag{2-6}$$

where $\zeta = \min(k,l)$. Figure 2-3 plots a typical discrete auto-correlation function of the chaotic series. In this case N is taken to be 500. As shown in the figure, there is a large peak at $(k-l) = 0$ and the function decays rapidly.

2.2.2.4 Discrete Cross-correlation Function

Assume that there are two chaotic series $\{x_n\}$ and $\{x'_n\}$ generated by the same map (2-5) but with different initial conditions. Define the discrete cross-correlation function of the series $\{x_n\}$ and $\{x'_n\}$, with a relative time shift of $k-l$ units, as

$$\theta_{xx'}(k,l) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=-\zeta}^{N-1-\zeta} x_{k+n} x'_{l+n} \tag{2-7}$$

where ζ is defined as in the previous section. Figure 2-4 plots a typical discrete cross-correlation function of the chaotic series with N taken to be 500. The initial conditions of the two series are 0.127 and 0.531 respectively. As shown in the figure, the discrete cross-correlation function remains more or less constant. Moreover, due to the fact that dc components exist in the two series, the discrete cross-correlation function has a non-zero average value.

2.2.2.5 Wideband

To evaluate the power spectral density (psd) of the chaotic series, a fast Fourier transform is performed on the discrete auto-correlation function in Figure 2-3 and the result is plotted in Figure 2-5. As shown in the figure, the psd of the chaotic signal occupies a very wide spectrum. Except the dc component which is particular strong (cannot be displayed on the same diagram because it equals 256), all other frequency components are of similar order of magnitude.

2.3 Chaos for Communications

In the previous section, the properties of chaos in general have been discussed. However, chaotic signals derived from different maps or differential equations also have their own distinct features. So when chaos is applied to communications, are all chaotic signals equally suitable and effective? What features should a chaotic signal possess in order to establish an effective and practical communications link?

2.3.1 Criteria

In a conventional direct sequence spread spectrum communications system, spreading codes of ± 1 are used to spread the binary symbols ± 1. As a result, after spreading, the spread signal consists of ± 1 too. So, to minimize any unnecessary change to the post-modulation functional blocks, the chaotic signal should be generated with a map on $[-1,+1]$.

Furthermore, for a spreading code, the probabilities of occurrences of $+1$ and -1 are nearly the same, rendering the average value of the spreading code to be nearly zero. As such, no power will be spent on transmitting any dc component, which does not carry any information. Hence, the average value of the chaotic signal should ideally be zero. For example, if the probability density function (pdf) of the chaotic signal is symmetrical along the y-axis, it will produce a zero average value to the signal.

Since all chaotic signals are bounded, we can always use scaling combined with dc-level adjustment to ensure the output lies within $[-1,+1]$. However, the symmetrical pdf property or zero average value is not guaranteed.

2.3.2 Features of Some Simple Maps

Four relatively simple maps — tent map, logistic map, cubic map, and Hénon map [Alli 96], [Deva 92], [Mull 93] — have been investigated to check their feasibilities as a chaos generator in communications. The equations of the maps are listed in Table 2-1. Assume that the chaotic series $\{x_n\}$ is generated by the map $x_{n+1} = g(x_n)$. For each of the four maps, an appropriate initial condition is chosen and the map is iterated 10^5 times. The distribution of the numbers in the series is plotted in Figures 2-6 to 2-9.

Figures 2-6 and 2-7 show that the domains of the tent map and logistic map are both [0,+1]. Moreover, the distribution of the numbers for the tent map is quite uniform within the domain. For the logistic map, the distribution is symmetrical along the x=0.5 line. The numbers also tend to cluster around the edges of the domain. In fact, there are over 2000 occurrences in each case that the iterated value is larger than 0.999 or below 0.001. On the other hand, the domain of the cubic map is [−1,+1] and the distribution of the numbers is symmetrical along the y-axis. Similar to the logistic map, the numbers tend to cluster around the edges of the domain and there are about 1400 occurrences in each case that the number is larger than 0.999 or below –0.999. For the Hénon map, the domain for $\{x_n\}$ is [−1.25,+1.28] and no symmetry is found in the distribution. Based on the above observations, among the four maps studied, only the cubic map can provide a domain within [−1,+1] as well as a symmetrical pdf along the y-axis. As a consequence, we have selected the cubic map as the chaos generator in our study of chaos-based digital communications systems. Next we shall look at some characteristics of the cubic map which will be useful in the chapters that follow.

2.3.3 Properties of the Cubic Map

2.3.3.1 Domain

As shown in the previous section, the domain of the cubic map is [–1,+1]. Hence starting with an initial condition in this region, we can be sure that the series $\{x_n\}$ will lie within the region forever.

2.3.3.2 Initial conditions

Different initial conditions may give rise to different kinds of orbits. Given the initial conditions are selected within the domain [–1,+1], we can divide the orbits of the series $\{x_n\}$ into several categories.

Fixed Points

If the initial condition equals to one of the fixed points, the system will stay at the fixed point forever. Under such circumstances, the following equation must hold:

$$x_0 = 4x_0^3 - 3x_0 \Leftrightarrow 4x_0^3 - 4x_0 = 0 \Leftrightarrow x_0 = 0, \pm 1.$$

Therefore, initial conditions of 0 or ±1 will not drive the system into chaos but ensure that the system stays at the stable points 0 or ±1.

Eventually Fixed Points

Such initial conditions are not fixed points. However, with any of these initial conditions, the system will converge to one of the fixed points after a number of iterations. For example, assume that the system converges to one of the fixed points after one iteration, i.e. $4x_0^3 - 3x_0 = 0, \pm 1$.

Case I. $4x_0^3 - 3x_0 = 0 \Rightarrow (4x_0^2 - 3)x_0 = 0 \Rightarrow x_0 = 0, \pm\frac{\sqrt{3}}{2}$.

Case II. $4x_0^3 - 3x_0 = 1 \Rightarrow 4x_0^3 - 3x_0 - 1 = 0 \Rightarrow x_0 = -0.5, \frac{1 \pm \sqrt{5}}{2}$.

Case II. $4x_0^3 - 3x_0 = -1 \Rightarrow 4x_0^3 - 3x_0 + 1 = 0 \Rightarrow x_0 = 0.5, \frac{-1 \pm \sqrt{5}}{2}$.

0 is a fixed point itself and hence it is not counted. Out of the other 8 initial conditions, only ±0.5 are rational. For the other 6 irrational numbers, their exact values cannot be stored or used in modern computers where numbers are represented by a finite number of digits. As a consequence, initial conditions of ±0.5 should be avoided if it is required to drive the system into chaos.

Periodic Orbits

Such conditions will repeat itself after a number of iterations. In other words, the system is oscillating between a number of points. For example if the initial condition has a period of 2, we have $x_1 = 4x_0^3 - 3x_0$ and $x_0 = x_2 = 4x_1^3 - 3x_1$. Substitute the expression of x_1 into the other equation, we obtain $32x_0^9 - 72x_0^7 + 54x_0^5 - 15x_0^3 + x_0 = 0$. Solving the equation gives the solutions $x_0 = 0, \pm 1, \pm\frac{1}{\sqrt{2}}, \pm\sqrt{\frac{3+\sqrt{5}}{8}}, \pm\sqrt{\frac{3-\sqrt{5}}{8}}$. Except 0 or ±1, which are actually fixed points, all other values are irrational which cannot be represented in digital computers.

Eventually Periodic Orbits

These initial conditions do not lie on any periodic orbit. However, under such initial conditions, the system will eventually be driven into a periodic orbit after a number of iterations.

Chaotic Orbits

Such initial conditions will drive the system into chaos. From the above analysis, initial conditions of 0, ±0.5 and ±1 must not be used. In all our simulations, arbitrary numbers within [−1,+1], except 0, ±0.5 and ±1, are first selected as the initial conditions. To further ensure that chaos is generated, for each of the initial conditions used, the last 100 numbers created by the map will be inspected to check that the series does not fall into any periodic orbit or converge to any of the fixed points. One typical chaotic series, generated with an initial condition of 0.07, is plotted in Figure 2-10 where the 200th to 300th numbers are shown. As expected, there is no periodic pattern detected.

2.3.3.3 Probability Density Function

With an initial condition of 0.07, the cubic map is iterated 100,000 times. The pdf of the iterated value is plotted in Figure 2-11. As mentioned in Section 2.3.2., it can be observed that the distribution is symmetrical along the y-axis. That is to say, the average value of the chaotic series should be zero. Moreover, the distribution is quite even between [−0.75, +0.75] while in the regions [−1, −0.75] and [0.75, 1], the probability gets higher when the value approaches −1 or +1. Such distribution can also be observed in Figure 2-10, where there is a large proportion of points with amplitudes approaching ±1. Since there is a high probability that the output gives a larger output, the average output power will be larger when the chaotic series is used to represent the binary data.

2.3.3.4 Discrete Auto-correlation Function and Power Spectral Density

The discrete auto-correlation function of a typical chaotic series generated by the cubic map is plotted in Figure 2-12. It is found that shifting the series by as little as one time step will produce two nearly uncorrelated sequences. When there is no time shift, the auto-correlation function approximately equals 0.5, which is also the average power of the signal.

The power spectral density of the series, obtained by taking the discrete Fourier transform of the auto-correlation function, is depicted in Figure 2-13. The power of the chaotic series is found to spread over a large bandwidth with no significantly large components. Since the power is spread over such a large bandwidth, each frequency component will have a very small power. Therefore, if the chaotic series is to carry information, which has a smaller bandwidth, the modulated signal will occupy the same bandwidth as the chaotic sequence. As a consequence, the resultant signal, having much lower psd, will not be easily noticed by others, especially by unwanted opponents.

2.3.3.5 Discrete Cross-correlation Function

The discrete cross-correlation function between chaotic series with initial conditions 0.07 and 0.17 respectively have been evaluated by simulation. A typical graph is shown in Figure 2-14. It can be observed that there is a very low cross-correlation value between sequences generated with different initial conditions.

2.3.4 Properties of Chaotic Series of Finite Length

In the previous section, we have discussed the properties of chaotic series generated by the cubic map. In chaos-based digital communications, however, only a

finite length of the chaotic sequence will be used to represent a binary symbol. Therefore, the auto-correlation and cross-correlation properties of the finite length sequences could be quite different from those of infinite sequences. To facilitate the study of chaos-based digital communications systems under a noisy environment, we also investigate the cross-correlation between chaotic sequences of finite length and normal random sequences of the same length. 10 initial conditions have been selected and for each of them, more than 10^7 iterations have been performed to create the chaotic series used for the analyses below.

2.3.4.1 Partial Discrete Auto-correlation Function

To facilitate the evaluation of the auto-correlation of chaotic sequence samples of finite length, we define the partial discrete auto-correlation function of the chaotic series $\{x_n\}$ as

$$\gamma_x(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n}x_{l+n} \tag{2-8}$$

where L is the length of the chaotic sequence samples and k, $l \geq 0$. The function $\gamma_x(k,l,L)$ depends on k, l, L as well as the initial condition of the series. Extensive computer simulations (Appendix A) have been performed to find out the statistical properties of $\gamma_x(k,l,L)$. Two values of L have been considered, L=100 and L=1000. The analysis is further divided into two cases — k= l and $k \neq l$.

Case I. $k = l$

Equation (2-8) now becomes

$$\gamma_x(k,k,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n}^2 \,. \tag{2-9}$$

$\gamma_x(k,k,L)$ is equivalent to the mean-squared value of the chaotic sequence samples. For a fixed L, $\gamma_x(k,k,L)$ varies because of the non-periodic nature of chaos. As shown in Appendix A, extensive computer simulations show that $\gamma_x(k,k,L)$ follows a normal distribution with mean $m_{x,k=l} = 0.5$. The variances for L=100 and L=1000 are $\sigma^2_{x,k=l} = 1.24\text{x}10^{-3}$ and $\sigma^2_{x,k=l} = 1.24\text{x}10^{-4}$ respectively.

Case II. $k \neq l$

In this case, there is very low correlation between the two chaotic samples. Simulation results (Appendix A) show that $\gamma_x(k,l,L)$ follows a normal distribution with zero mean and variances $\sigma^2_{x,k\neq l} = 2.5\text{x}10^{-3}$ and $\sigma^2_{x,k\neq l} = 2.5\text{x}10^{-4}$ for L=100 and L=1000 respectively.

2.3.4.2 Partial Discrete Cross-correlation Function

We define the partial discrete cross-correlation function between the chaotic series $\{x_n\}$ and $\{x'_n\}$ as

$$\gamma_{xx'}(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n} x'_{l+n} \tag{2-10}$$

where L is the length of the chaotic sequence samples and k, $l \geq 0$. Extensive computer simulations (Appendix B) show that $\gamma_{xx'}(k,l,L)$ follows a normal distribution with

zero mean and variances $\sigma^2_{xx'} = 2.50\text{x}10^{-3}$ and $\sigma^2_{xx'} = 2.50\text{x}10^{-4}$ for L=100 and L=1000 respectively.

In fact, the distribution of the partial discrete cross-correlation function is the same as that of the partial discrete auto-correlation function where $k \neq l$. Therefore, for any two unequal chaotic samples of length L, taken from different locations of the same chaotic series or from two different chaotic series, the correlation between them is normally distributed with zero mean and a variance dependent on the length L.

2.3.4.3 Partial Discrete Cross-correlation Function between Chaotic Series and Normal Random Sequences

Define a normal random sequence $\Phi = \{\phi_0, \phi_1, \phi_2, \phi_3, \phi_4, ...\}$, the elements of which are normal random variables with zero mean and unit variance. The partial discrete cross-correlation function between the chaotic series $\{x_n\}$ and the normal random sequence $\{\phi_n\}$ is defined as

$$\gamma_{x\phi}(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n}\phi_{l+n} \cdot \tag{2-11}$$

As shown in Appendix C, computer simulations show that $\gamma_{x\phi}(k,l,L)$ is normally distributed with zero mean and variances $\sigma^2_{x\phi} = 5.0\text{x}10^{-3}$ and $\sigma^2_{x\phi} = 5.0\text{x}10^{-4}$ for L=100 and L=1000 respectively. As a consequence, given a normal random sequence $\Lambda = \{\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, ...\}$, the elements of which are normal random variables with zero mean and variance σ^2_λ, the partial discrete cross-correlation function

$$\gamma_{x\lambda}(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n}\lambda_{l+n} \tag{2-12}$$

will follow a normal distribution with zero mean and variances $\sigma_{x\lambda}^2 = \sigma_{x\phi}^2\sigma_\lambda^2 = 5.0\text{x}10^{-3}\sigma_\lambda^2$ and $\sigma_{x\lambda}^2 = 5.0\text{x}10^{-4}\sigma_\lambda^2$ for L=100 and L=1000 respectively.

Table 2-2 summarizes the statistical properties of the partial discrete correlation functions in this section.

2.4 Conclusions

In this chapter, we have described how chaos is generated from a dynamical system. Properties of chaos such as aperiodic and sensitive to initial conditions are illustrated. To minimize any unnecessary change to the post-modulation functional blocks in conventional spread spectrum communications systems, the chaotic signal should be chosen such that the domain lies within [−1,+1]. Moreover, to ensure no power will be spent on transmitting any dc component, which does not carry any information, the average value of the chaotic signal should ideally be zero. This can be achieved if the probability density function of the chaotic signal possesses symmetry along the y-axis. Four relatively simple maps, namely tent map, logistic map, cubic map, and Hénon map, have been investigated and it is found that only cubic map possesses the properties mentioned above. Hence, the cubic map has been chosen as the chaos generator in our study of chaos-based digital communications systems and the general properties of the cubic map are then presented.

In chaos-based digital communications, only a finite length of the chaotic sequence will be used to represent a binary symbol. As a consequence, the partial discrete correlation properties of the cubic map have been fully investigated by using extensive computer simulations. It has been found that the mean-squared value of a chaotic sample of length L follows a normal distribution with mean 0.5 and variance dependent on L. For any two unequal chaotic samples, taken from different locations of the same chaotic series or from two different chaotic series, the correlation between them is normally distributed with zero mean and a variance dependent on the length L. The partial discrete cross-correlation function between the chaotic series and a normal random sequence, moreover, is normally distributed with zero mean, and a variance dependent on the length L as well as the variance of the random sequence. In general, the longer the length L, the smaller the variances will be in all cases.

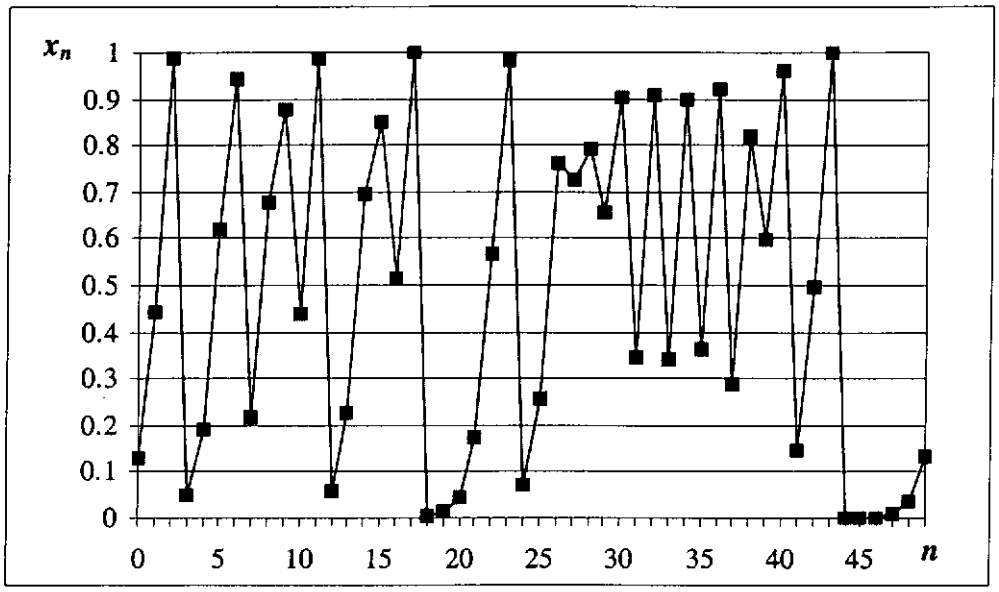


Figure 2-1 A plot of x_n against n for the logistic map

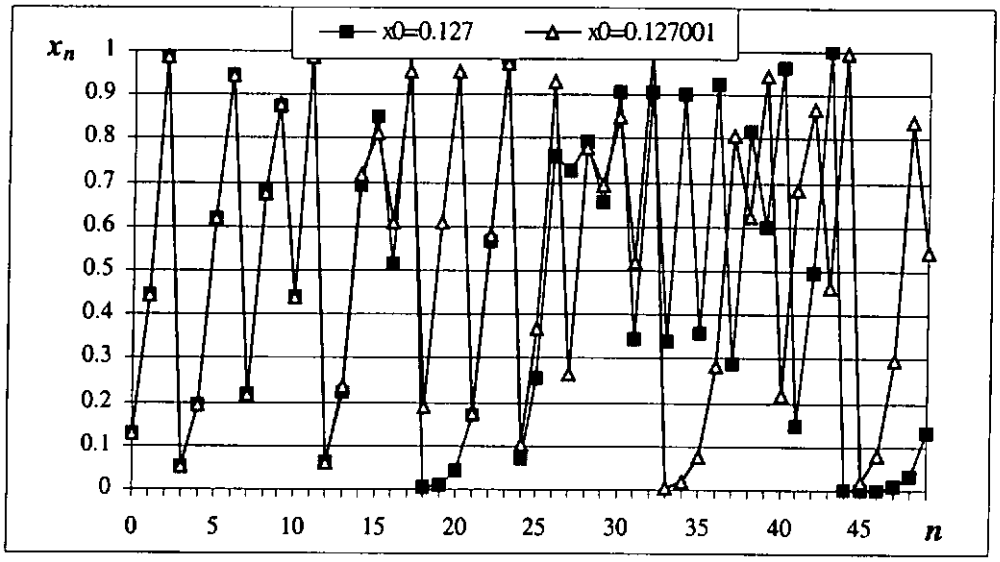


Figure 2-2 A plot of x_n against n for two slightly different initial conditions

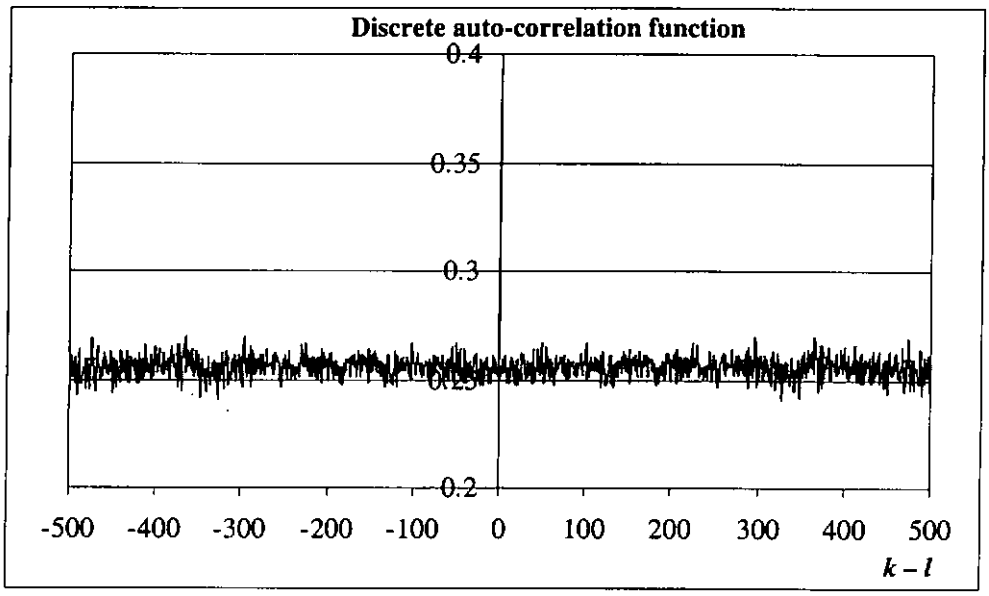


Figure 2-3 Discrete auto-correlation function of the chaotic series

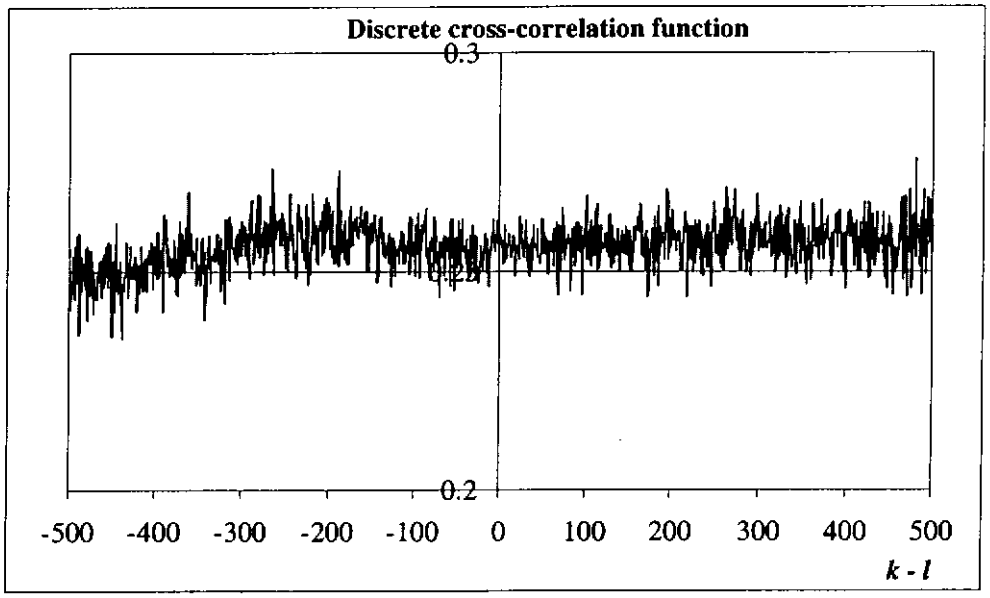


Figure 2-4 Discrete cross-correlation function of the chaotic series

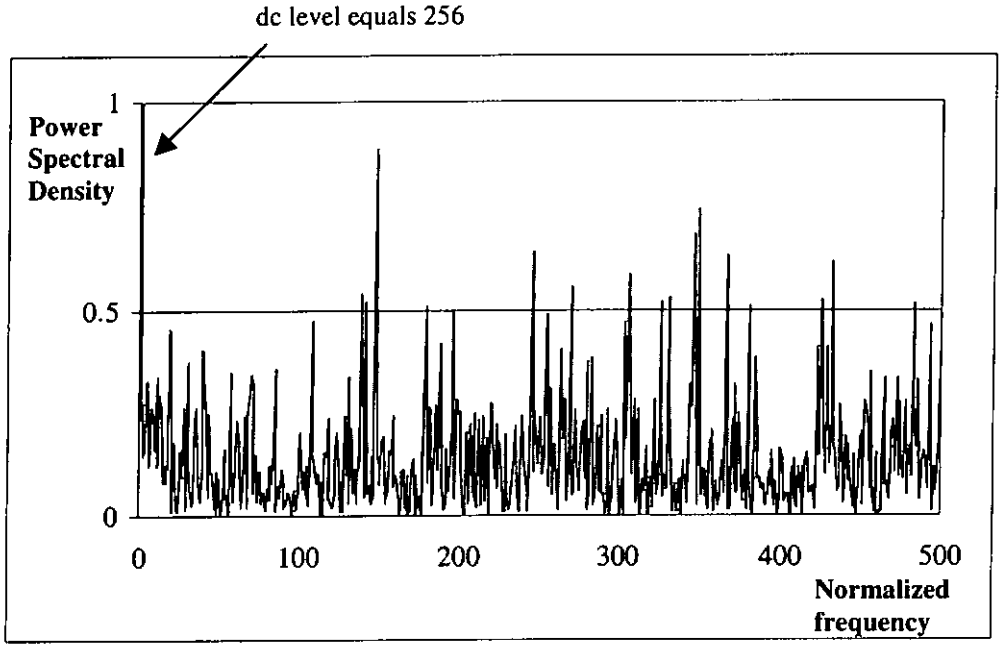


Figure 2-5 Power spectral density of a chaotic signal

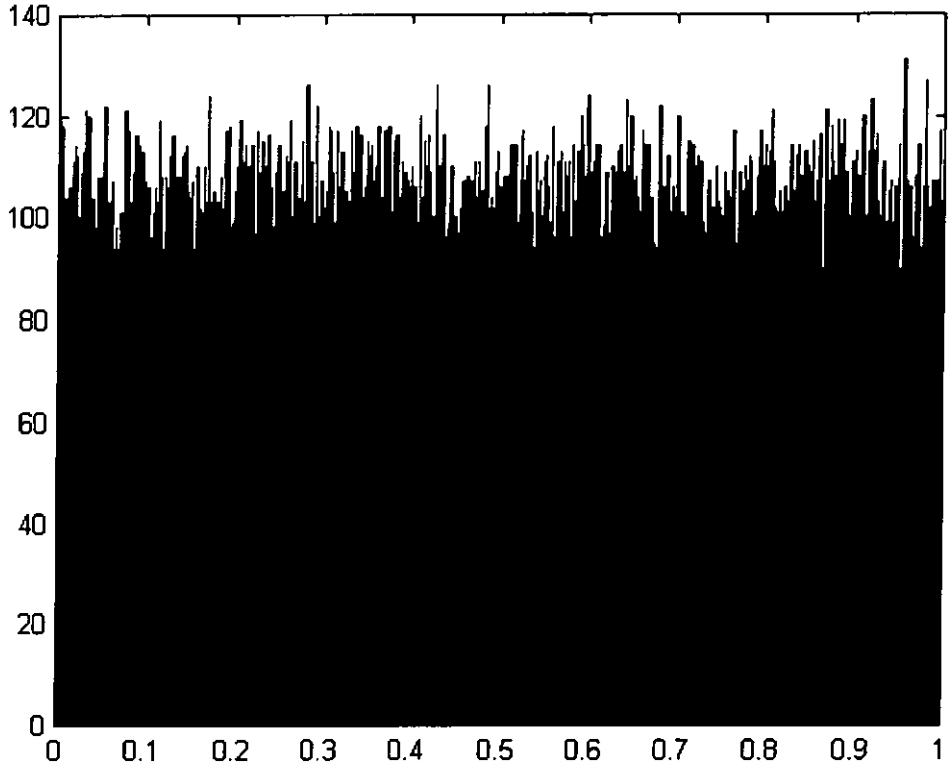


Figure 2-6 Distribution of numbers in the series generated by the tent map. The map is iterated 10^5 times. The interval [0,1] is divided into 1000 small intervals.

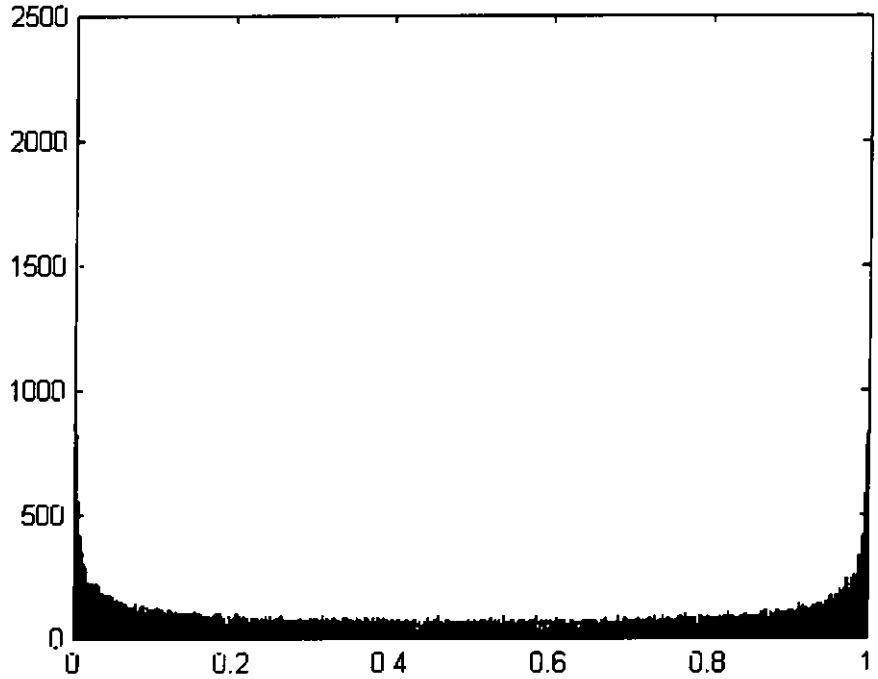


Figure 2-7 Distribution of numbers in the series generated by the logistic map. The map is iterated 10^5 times. The interval [0,1] is divided into 1000 small intervals.

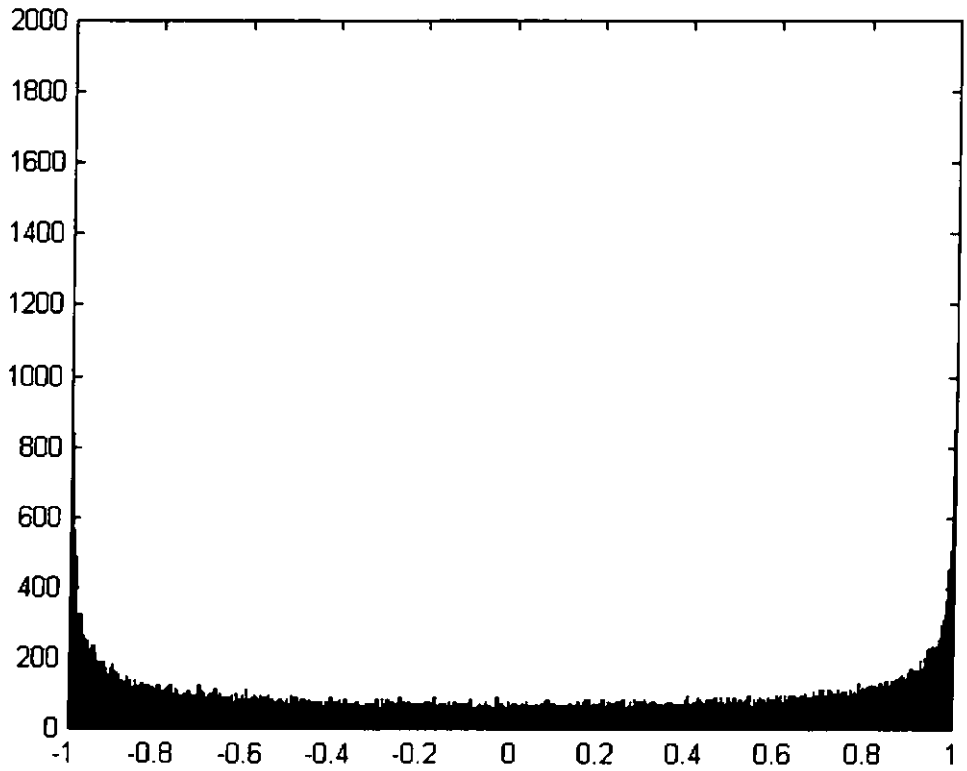


Figure 2-8 Distribution of numbers in the series generated by the cubic map. The map is iterated 10^5 times. The interval [–1,+1] is divided into 1000 small intervals.

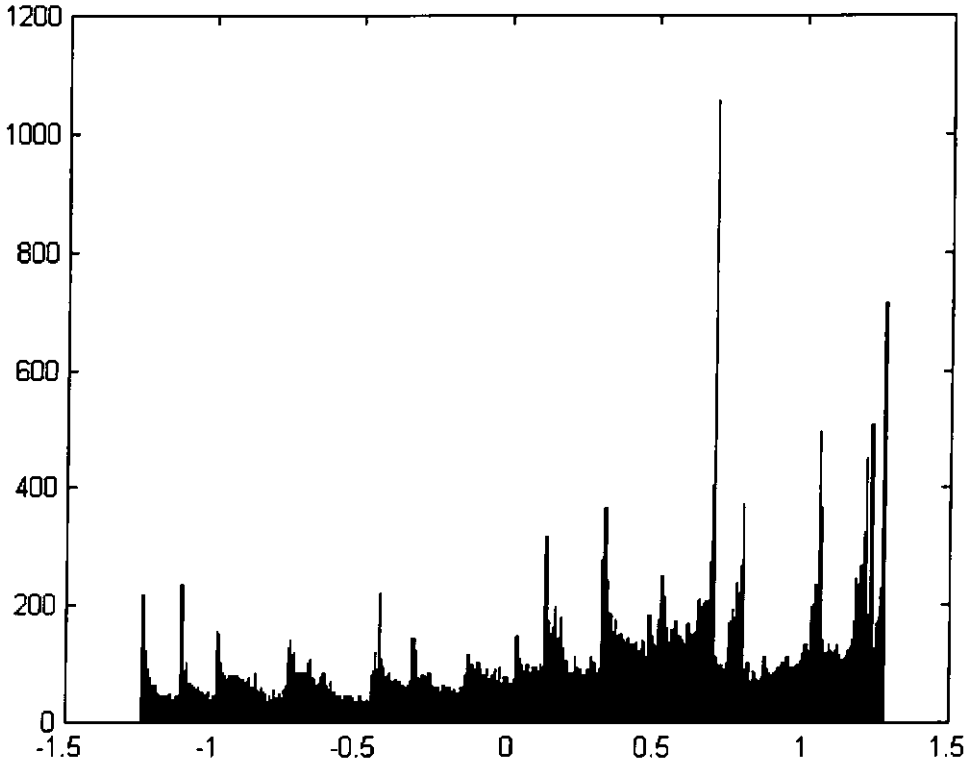


Figure 2-9 Distribution of numbers in the series generated by the Hénon map. The map is iterated 10^5 times. The interval [–1.5,1.5] is divided into 1000 small intervals.

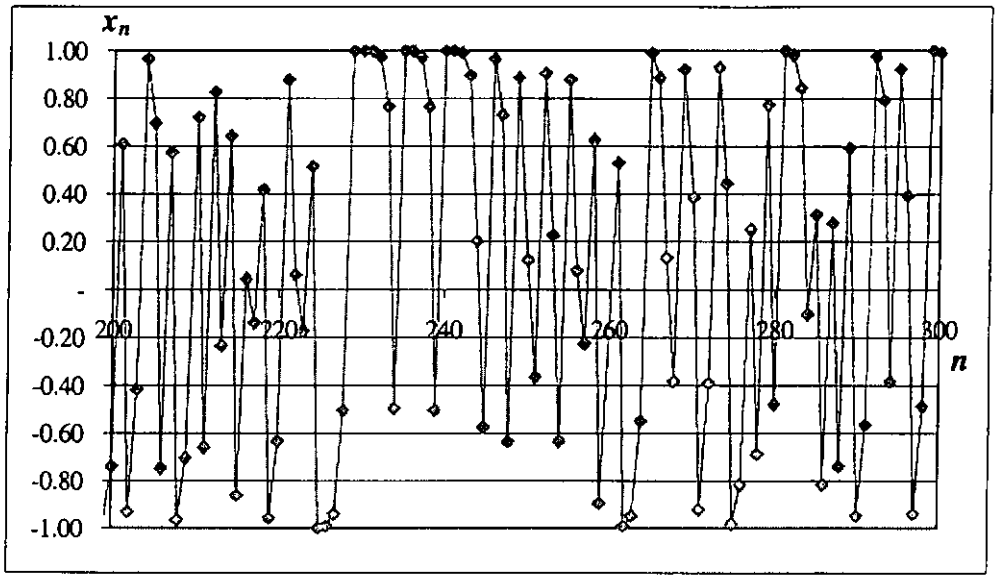


Figure 2-10 A plot of x_n against n for the cubic map with an initial condition of 0.07

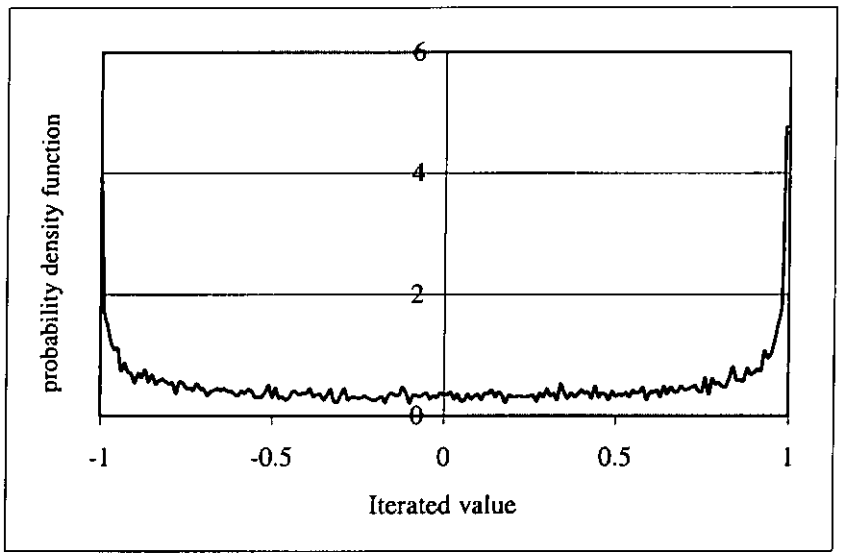


Figure 2-11 The pdf of the iterated value generated by the cubic map with an initial condition of 0.07

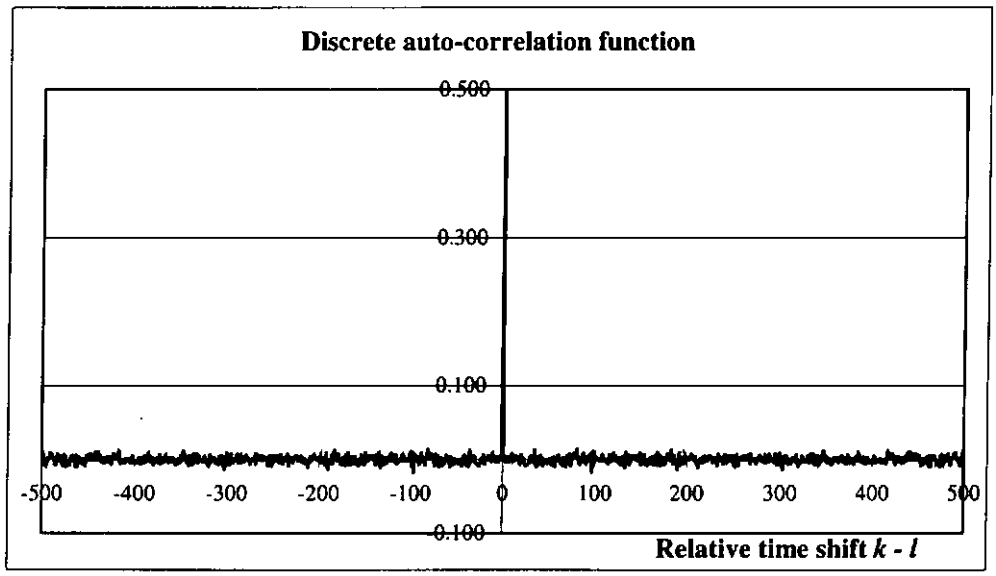


Figure 2-12 Discrete autocorrelation function of the chaotic sequence generated with an initial condition of 0.07

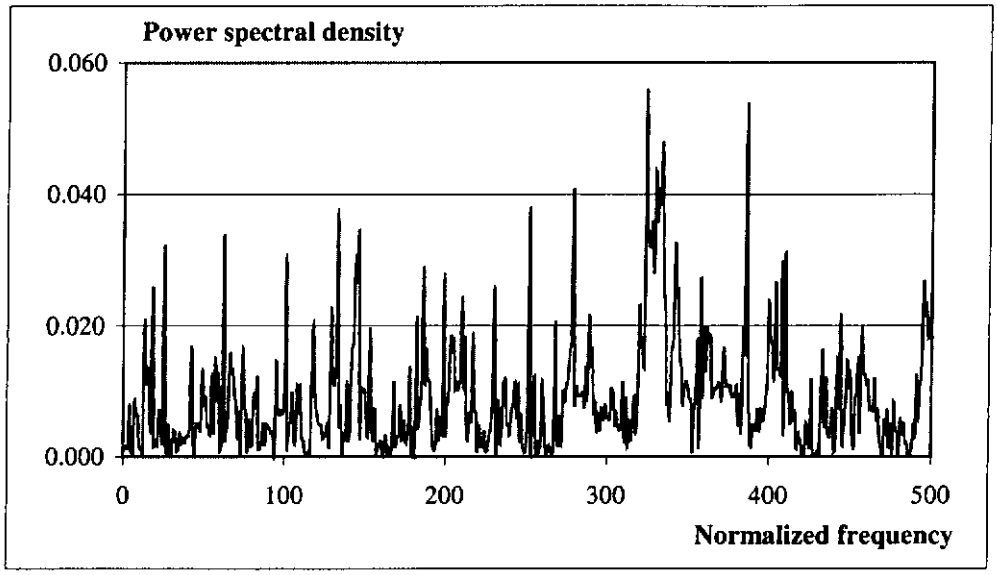


Figure 2-13 Power spectral density of the chaotic series generated with an initial condition of 0.07

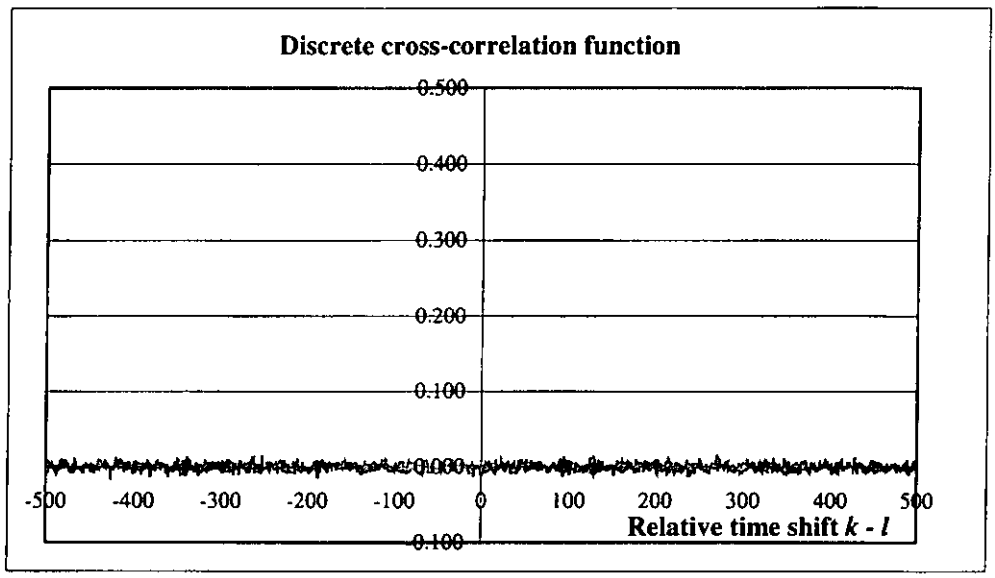


Figure 2-14 Discrete cross-correlation function of the chaotic sequences generated with initial conditions of 0.07 and 0.17

Map	***g*(.)**	**Domain**
Tent map	$x_{n+1} = \begin{cases} \dfrac{x_n}{0.6} & 0 \le x_n \le 0.6 \\ \dfrac{1-x_n}{0.4} & 0.6 < x_n \le 1 \end{cases}$	[0,+1]
Logistic map	$x_{n+1} = 4x_n(1-x_n)$	[0,+1]
Cubic map	$x_{n+1} = 4x_n^3 - 3x_n$	[−1,+1]
Hénon map	$x_{n+1} = y_n + 1 - 1.37x_n^2$ $y_{n+1} = 0.3x_n$	[−1.25,1.28]

Table 2-1 Table of maps

Type of partial discrete correlation function	Correlation function	Mean	Variance
Auto-correlation with $k=l$	$\gamma_x(k,k,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}^2$	$m_{x,k=l}=\begin{cases}0.5 & L=100\\ 0.5 & L=1000\end{cases}$	$\sigma_{x,k=l}^2=\begin{cases}1.24\text{x}10^{-3} & L=100\\ 1.24\text{x}10^{-4} & L=1000\end{cases}$
Auto-correlation with $k\neq l$	$\gamma_x(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}x_{l+n}$	$m_{x,k\neq l}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{x,k\neq l}^2=\begin{cases}2.50\text{x}10^{-3} & L=100\\ 2.50\text{x}10^{-4} & L=1000\end{cases}$
Cross-correlation	$\gamma_{xx'}(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}x'_{l+n}$	$m_{xx'}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{xx'}^2=\begin{cases}2.50\text{x}10^{-3} & L=100\\ 2.50\text{x}10^{-4} & L=1000\end{cases}$
Cross-correlation with normal random sequences with zero mean and unit variance	$\gamma_{x\phi}(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}\phi_{l+n}$	$m_{x\phi}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{x\phi}^2=\begin{cases}5.0\text{x}10^{-3} & L=100\\ 5.0\text{x}10^{-4} & L=1000\end{cases}$
Cross-correlation with normal random sequences with zero mean and variance σ_λ^2	$\gamma_{x\lambda}(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}\lambda_{l+n}$	$m_{x\lambda}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{x\lambda}^2=\begin{cases}5.0\text{x}10^{-3}\sigma_\lambda^2 & L=100\\ 5.0\text{x}10^{-4}\sigma_\lambda^2 & L=1000\end{cases}$

Table 2-2 Means and variances of the partial discrete correlation functions of the chaotic series

CHAPTER 3

CHAOS-BASED DIGITAL MODULATION

Ever since Carroll and Pecora have demonstrated the synchronization of chaotic circuits in 1991 [Carr 91], much effort has been put into researching communications using chaos. In fact, chaos-based communications techniques emerged only in the last decade. As introduced in Chapter 1, chaos can be used in analog communications [Itoh 95], [Koca 92], digital communications [Jako 98], [Kenn 98a], [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a], [Kis 98b], [Kolu 97a], [Kolu 97b], [Kolu 98] as well as spread spectrum communications [Heid 94], [Mazz 97], [Mazz 98], [Sett 99]. In this chapter, several chaos-based digital modulation techniques will be reviewed. Note that only the baseband models have been considered here. The conversions between bandpass systems and lowpass equivalent models can be found in [Kolu 98], [Proa 94].

3.1 Introduction

In a digital communications system, the information to be transmitted is mapped by the modulator to an analog sample function before passing to the analog channel. Due to the limitations of the channel such as attenuation, bandpass filtering and noise, the received signal is a corrupted version of the transmitted sample. Based on this corrupted sample, the demodulator has to estimate the transmitted symbol.

In a conventional digital communications system [Proa 94],[Proa 95], the analog sample functions differ by phase (phase shift keying PSK), frequency (frequency shift keying FSK) or amplitude (amplitude shift keying ASK). The receiver detects such differences and decodes the received signal. For the same transmitted symbol, the same analog sample is transmitted. In coherent detection, a replica of the basis functions is reproduced at the receiver to aid the demodulation. It is assumed that by synchronization, the basis functions can be recovered from the corrupted received signal. In noncoherent detection, the basis functions need not be recovered at the receiver. For example, in differential PSK, demodulation is achieved by comparing the received signal in any given signaling interval to the phase of the received signal from the preceding signaling interval.

In chaos-based digital communications systems, the analog chaotic samples are never the same due to the nonperiodic nature of chaos. Coherent demodulation is always possible provided that the receiver can reproduce the chaotic signals accurately. On the other hand, since the correlation between different chaotic samples is low, conventional differential encoding/decoding techniques may not be suitable. Hence, to decode the signal using noncoherent detection, certain property of the received sample has to be estimated, such as the bit energy of the received signal, and compared with a threshold for detection. In the following sections, four chaos-based digital modulation schemes will be presented.

3.2 Chaos Shift Keying

Consider the Chaos Shift Keying (CSK) [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a] digital communications system shown in Figure 3-1, the transmitter consists of two

chaotic generators producing basis functions $c_{-1}(t)$ and $c_{+1}(t)$ respectively. If a binary "–1" is to be transmitted during the interval $[(m-1)T_b, mT_b)$, $c_{-1}(t)$ will be sent. On the other hand, if "+1" needs to be transmitted, $c_{+1}(t)$ is sent. Figure 3-2 depicts an example of the basis functions and the transmitted waveform $s(t)$. In this example, the chaotic signal generators produce rectangular pulses with chaotic amplitudes and width T_c =10μs. The bit duration used is T_b =100μs. After passing through the channel, the corrupted signal arrives at the input of the demodulator.

3.2.1 Coherent Demodulation

Figure 3-3 shows a coherent CSK demodulator. The two synchronization blocks try to recover the two chaotic signals $c_{-1}(t)$ and $c_{+1}(t)$ from the received corrupted sample $p(t)$. An acquisition time T_s is assumed for the synchronization blocks to lock to the incoming signal. The reproduced basis functions are then used to correlate with the received signal during the remainder of the bit duration. Afterwards, the outputs of the correlators are sampled and compared. The outputs of the correlators at the end of the mth symbol period are given by

$$\mathrm{Corr}_{-1}(mT_b) = \int_{(m-1)T_b+T_s}^{mT_b} p(t)\hat{c}_{-1}(t)dt \tag{3-1}$$

and $$\mathrm{Corr}_{+1}(mT_b) = \int_{(m-1)T_b+T_s}^{mT_b} p(t)\hat{c}_{+1}(t)dt\,. \tag{3-2}$$

The output of the adder at this time instant is

$$\begin{aligned} z(mT_b) &= \mathrm{Corr}_{+1}(mT_b) - \mathrm{Corr}_{-1}(mT_b) \\ &= \int_{(m-1)T_b+T_s}^{mT_b} p(t)c_{+1}(t)dt - \int_{(m-1)T_b+T_s}^{mT_b} p(t)c_{-1}(t)dt. \end{aligned} \tag{3-3}$$

If $z(mT_b)$ is larger than zero, a "+1" is decoded for the mth symbol. Otherwise, a "−1" is detected.

To simplify the analysis, we assume that the only defect of the channel is additive white Gaussian noise (AWGN). Moreover, the two chaotic signals can be re-generated perfectly at the receiver and the synchronization time is negligible compared with the bit period. Using the transmitted signal in Figure 3-2 as an example, Figures 3-4 and 3-5 shows the outputs of the correlators and the adder for large and small signal-to-noise ratios (SNRs) respectively. Note that errors do occur for small SNR. Detail derivation of the numerical bit error probability (BEP) and more simulation results will be shown in Chapter 4.

3.2.2 Noncoherent Demodulation

In coherent detection, it is assumed that the chaotic signals can be perfectly re-generated at the receiver. Such requirement, however, still remains as one of the most important challenges in chaos-based communications. In noncoherent CSK demodulation, the chaotic basis functions need not be recovered at the receiver. Only the bit energy is estimated and compared with a certain threshold for detection.

Chaotic signals with different bit energies are used to represent the binary data. If a binary "−1" is to be transmitted during the interval $[(m-1)T_b, mT_b)$, a chaotic sample function $c_{-1}(t)$ with mean bit energy $\overline{E_{-1}}$ is transmitted. On the other hand, if "+1" needs to be transmitted, a chaotic sample function $c_{+1}(t)$ with mean bit energy $\overline{E_{+1}}$ is radiated. There are two ways to generate chaotic signals with different bit energies. First, we can make use of different chaos generators. Second, the same chaos generator

is used but the output is multiplied by two different constants. Hence the binary information to be transmitted will be mapped to the bit energy of chaotic sample functions. Replace the CSK transmitter in Figure 3-1 by the one in Figure 3-6 and perform the simulation again, new basis functions and transmitted waveform are obtained, as shown in Figure 3-7. Note that Figure 3-7(a) and 3-7(b) are of the same shape but different by a factor of 2.

At the receiving end, the bit energy is estimated by a correlator, as shown in Figure 3-8. Assume that the only distortion on the signal is due to noise. That is to say, $p(t) = s(t) + n(t)$, where $n(t)$ is the noise signal. For the mth received symbol, the sampled output of the correlator, or equivalently the received bit energy E_{br}, is given by

$$\begin{aligned} E_{br} &= \int_{(m-1)T_b}^{mT_b} [p(t)]^2 dt \\ &= \int_{(m-1)T_b}^{mT_b} [s(t) + n(t)]^2 dt \\ &= \int_{(m-1)T_b}^{mT_b} s^2(t)dt + 2\int_{(m-1)T_b}^{mT_b} s(t)n(t)dt + \int_{(m-1)T_b}^{mT_b} [n(t)]^2 dt. \end{aligned} \tag{3-4}$$

In a high SNR environment, the second and third integrals are negligible compared with the first one. Therefore E_{br} equals to one of the two bit energies

$$E_{-1} = \int_{(m-1)T_b}^{mT_b} c_{-1}^2(t)dt \tag{3-5}$$

$$\text{or } E_{+1} = \int_{(m-1)T_b}^{mT_b} c_{+1}^2(t)dt\,. \tag{3-6}$$

In conventional modulation schemes, the bit energies are the same for the same transmitted symbol. However, in CSK, the chaotic signals, being non-periodic, give varying bit energies even for the same transmitted symbol. Figure 3-9 shows a typical histogram of samples of the correlator output under a high SNR environment. Note that

E_{br} does not produce two distinct values. Instead, E_{br} clusters around the two mean bit energies $\overline{E_{-1}}$ and $\overline{E_{+1}}$ with variances $\sigma^2_{E_{-1}}$ and $\sigma^2_{E_{+1}}$, respectively. The variances can be reduced by increasing the bit duration T_b. By setting the threshold to be somewhere midway between $\overline{E_{-1}}$ and $\overline{E_{+1}}$, the received symbols can be decoded correctly.

For a low SNR environment, the second and third terms in equation (3-4) cannot be ignored. The second integral can be positive or negative while the third one always produces positive output. Hence the output E_{br} will be increased significantly compared with the high SNR case. Figure 3-10 shows the histogram of E_{br} in a noisy environment. In this case, the output of the correlator is increased and the two distinct bit-energy regions in Figure 3-9 overlap. Hence no matter where we set the threshold, errors are bound to occur. An optimal threshold can be set so as to minimize the bit error probability. However, it is dependent on the signal-to-noise ratio (SNR). This, as a consequence, poses a significant drawback of noncoherent CSK.

3.3 Chaotic On-Off-Keying

In CSK, two chaotic signals are used to represent the two binary symbols. The separation between the two mean bit energies $\overline{E_{-1}}$ and $\overline{E_{+1}}$ is given by

$$\overline{E_{\text{sep}}} = |\overline{E_{-1}} - \overline{E_{+1}}| \tag{3-7}$$

and the average transmitted bit energy of the system is

$$\overline{E_{bt}} = (\overline{E_{-1}} + \overline{E_{+1}})/2 . \tag{3-8}$$

To maximize the separation between the two detected symbols at the receiver for a given average bit energy, Chaotic On-Off-Keying (COOK) is proposed in [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a].

In COOK, only one chaotic signal is required. As shown in Figure 3-11, to transmit a "–1", the switch is closed. Otherwise, it is opened for the bit duration. Therefore the transmitted signal is given by

$$s(t) = \begin{cases} 0 & \text{"+1" is transmitted} \\ c_{-1}(t) & \text{"−1" is transmitted.} \end{cases} \tag{3-9}$$

The structure of a COOK receiver is the same as the noncoherent CSK receiver. Moreover, the analysis of the demodulation of COOK under a noisy environment is similar to that of noncoherent CSK, except that equation (3-6) is now modified to

$$E_{+1} = \int_{(m-1)T_b}^{mT_b} c_{+1}^2(t)dt = 0. \tag{3-10}$$

Histograms of the correlator output are plotted in Figures 3-12 and 3-13 under noiseless and noisy conditions respectively. Although COOK gives a better performance than CSK under the same environment, the optimal threshold is still dependent on the SNR.

3.4 Differential CSK

In both noncoherent CSK and COOK, the optimal threshold in the detector varies with the noise level. To overcome such threshold level shift problem, differential CSK (DCSK), which also allows noncoherent detection, is proposed [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a]. The advantage of DCSK over CSK and COOK is that the threshold level is always set at zero and is independent of the noise effect. Figure 3-14 shows the transmitter of a DCSK modulator. In DCSK, every transmitted symbol is

represented by two chaotic signal samples. The first one serves as the reference (reference sample) while the second one carries the data (data sample). If a "+1" is to be transmitted, the data sample will be identical to the reference sample, and if a "−1" is to be transmitted, an inverted version of the reference sample will be used as the data sample. Thus, for the mth symbol,

$$s(t) = \begin{cases} c(t) & (m-1)T_b \le t < (m-\frac{1}{2})T_b \\ c(t-\frac{T_b}{2}) & (m-\frac{1}{2})T_b \le t < mT_b \end{cases} \tag{3-11}$$

if "+1" is to be transmitted and

$$s(t) = \begin{cases} c(t) & (m-1)T_b \le t < (m-\frac{1}{2})T_b \\ -c(t-\frac{T_b}{2}) & (m-\frac{1}{2})T_b \le t < mT_b \end{cases} \tag{3-12}$$

if "−1" is to be transmitted. Figure 3-15 shows a typical waveform of $s(t)$.

At the receiver, the incoming signal is correlated with a delayed version of itself, as shown in Figure 3-16. For the mth received symbol, the output of the correlator gives

$$z(mT_b) = \int_{(m-\frac{1}{2})T_b}^{mT_b} p(t)p(t-\frac{T_b}{2})dt. \tag{3-13}$$

Assume that distortion to the transmitted signal is due to noise alone. Equation (3-13) is now re-written as

$$\begin{aligned} z(mT_b) &= \int_{(m-\frac{1}{2})T_b}^{mT_b} [s(t)+n(t)][s(t-\frac{T_b}{2})+n(t-\frac{T_b}{2})]dt \\ &= \int_{(m-\frac{1}{2})T_b}^{mT_b} s(t)s(t-\frac{T_b}{2})dt + \int_{(m-\frac{1}{2})T_b}^{mT_b} s(t)n(t-\frac{T_b}{2})dt \\ &+ \int_{(m-\frac{1}{2})T_b}^{mT_b} n(t)s(t-\frac{T_b}{2})dt + \int_{(m-\frac{1}{2})T_b}^{mT_b} n(t)n(t-\frac{T_b}{2})dt \end{aligned} \tag{3-14}$$

where $n(t)$ is the noise function at the input of the receiver. The first term gives a positive or negative value, depending on whether a "+1" or "−1" has been transmitted. For the other integral terms, it is obvious that their mean values are all zero. Therefore to optimize the bit error probability of the system, the threshold of the detector should be set at zero. As a consequence, the threshold of the detector is independent of the noise level.

Figure 3-17 depicts the output waveform of the correlator under a noiseless environment. Samples taken at multiples of T_b are then used to decode the binary symbols. Figure 3-18 shows the distribution of the correlator output under a high SNR environment. Note that the output values form two clusters at the two sides of the y-axis. A threshold of zero can clearly differentiate the two transmitted symbols. If the channel is noisy, the two clusters move closer together, as shown in Figure 3-19. As can be seen, the optimal threshold is still fixed at zero, though errors may occur inevitably. More detailed analyses will be shown in Chapter 5.

Another advantage of DCSK over CSK and COOK is that since both the reference and data samples are transmitted through the same channel, similar distortions are suffered by both samples provided that the channel does not vary much over the bit duration. Hence DCSK can be insensitive to the channel distortion. The main drawback of DCSK, however, is that it can only transmit half the data rate as the other systems because it spends half of the time transmitting the reference samples. One way to increase the data rate is to use a multilevel modulation scheme [Kolu 97a], but then, the receiver will be more complicated and the attenuation of the channel might also affect bit error performance.

3.5 Frequency Modulated DCSK

As shown in the previous histograms, the correlator outputs in the CSK, COOK and DCSK receivers vary from one bit to another even for the same transmitted symbol. It is due to the non-periodic nature of chaos that the bit energy of the transmitted symbol using CSK, COOK and DCSK varies from one bit to another. To produce a wideband chaotic signal with constant power, an appropriate chaotic signal is fed to a frequency modulator (FM modulator), as shown Figure 3-20. Then the output of the modulator will also be chaotic with a bandlimited power spectrum, the power spectral density of which is uniform [Kenn 99].

Replacing the chaotic signal generator in the DCSK transmitter in Figure 3-14 by the chaotic FM generator, Frequency Modulated DCSK (FM-DCSK) is obtained. The receiver structure of the demodulator is the same as the DCSK demodulator. The only difference is that the frequency modulated signals are directly correlated instead of the baseband chaotic signals. Figures 3-21 and 3-22 show the distribution of the correlator output in a FM-DCSK receiver. As expected, in the noiseless environment, there are only two possible values. In a noisy channel, a variation of output values appears. Note that as in the DCSK case, the threshold of the detector is always set at zero.

3.6 Conclusions

In this chapter, we have described the operations of four chaos-based digital modulation schemes, namely chaos shift keying (CSK), chaotic on-off-keying (COOK), differential CSK (DCSK), and frequency modulated DCSK (FM-DCSK). The block diagrams for the transmitters and receivers, together with some typical simulation results are also depicted.

CSK maps different binary symbols to outputs of different chaos generators. A coherent correlation CSK receiver is then used at the receiving end to decode the signals. Noncoherent detection is also feasible provided that the signals generated by the different generators have different attributes, such as mean of the absolute value, variance and standard deviation. In COOK, the chaotic signal is turned on/off by the binary data to be transmitted. Maximum distance between the elements of the binary symbols is then accomplished for a fixed average bit energy. A noncoherent detector is also possible in this case. In the noncoherent detection of both CSK and COOK, however, the decision level of the threshold detector depends on the signal-to-noise ratio. In DCSK, every transmitted symbol is represented by two chaotic signal samples. The first one is the reference sample while the second one is the data sample. Depending on the binary symbol to be transmitted, the data sample may be identical to or an inverted version of the reference sample. The advantage of DCSK over CSK and COOK is that the threshold level is always set at zero and is independent of the noise effect. Because of the non-periodic nature of chaos, the correlator outputs in the CSK, COOK and DCSK receivers vary from one bit to another, even for the same transmitted symbol under a noiseless environment. A bandlimited constant power chaotic signal is

produced by feeding an appropriately designed chaotic signal to an FM modulator. Combined with DCSK, it forms FM-DCSK. Besides having a fixed decision level of zero, the FM-DCSK receiver also gives the same correlator output for the same transmitted symbol under a noiseless environment.

In the next two chapters, we will investigate the performances of CSK and DCSK systems in a multi-user environment.

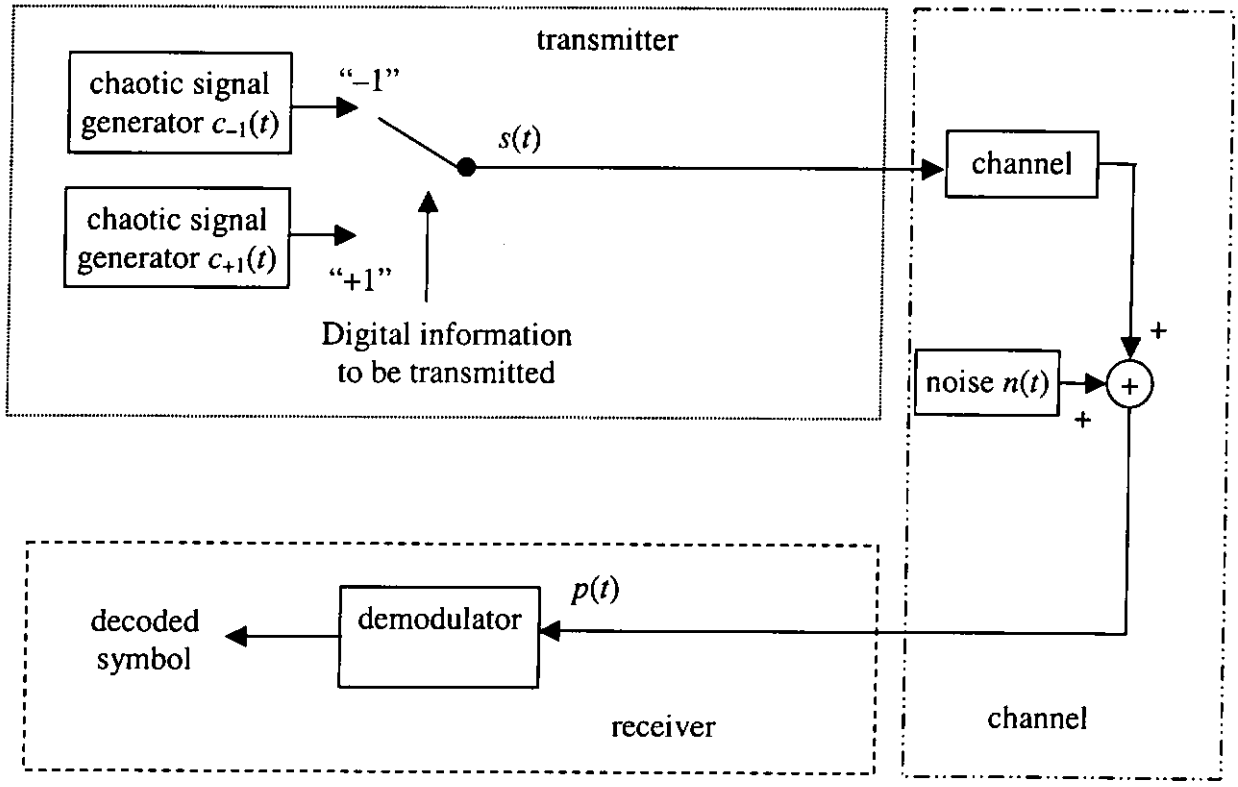


Figure 3-1 Chaos shift keying digital communications system

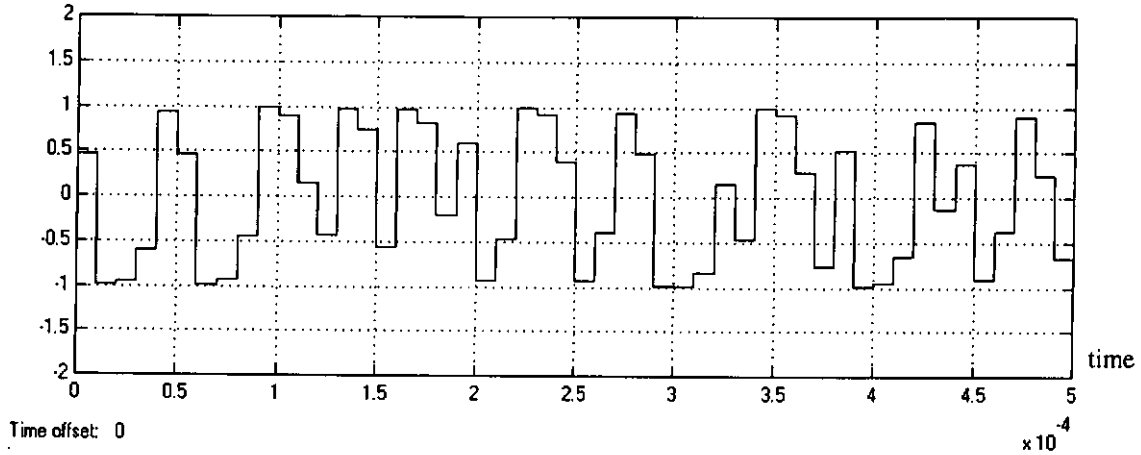


Figure 3-2(a) Basis function $c_{-1}(t)$ in a CSK communications system

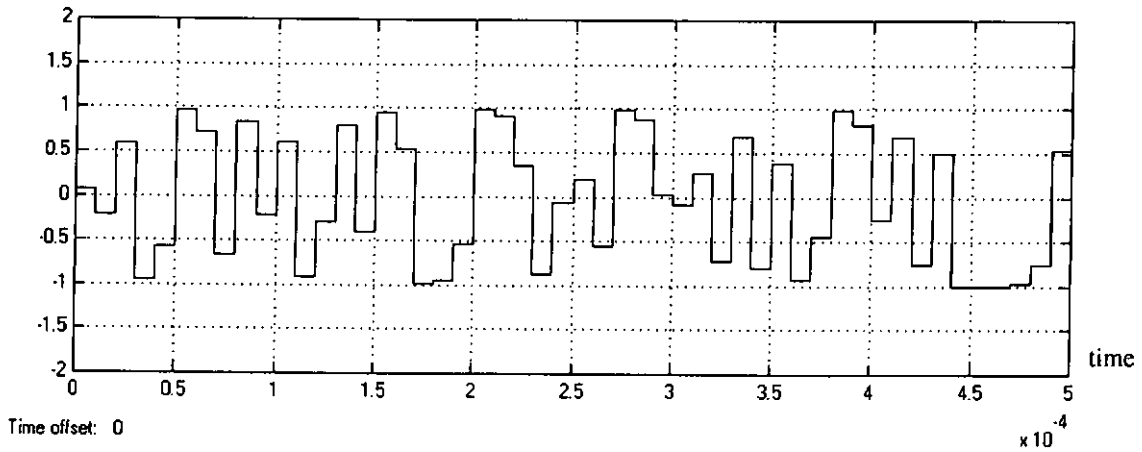


Figure 3-2(b) Basis function $c_{+1}(t)$ in a CSK communications system

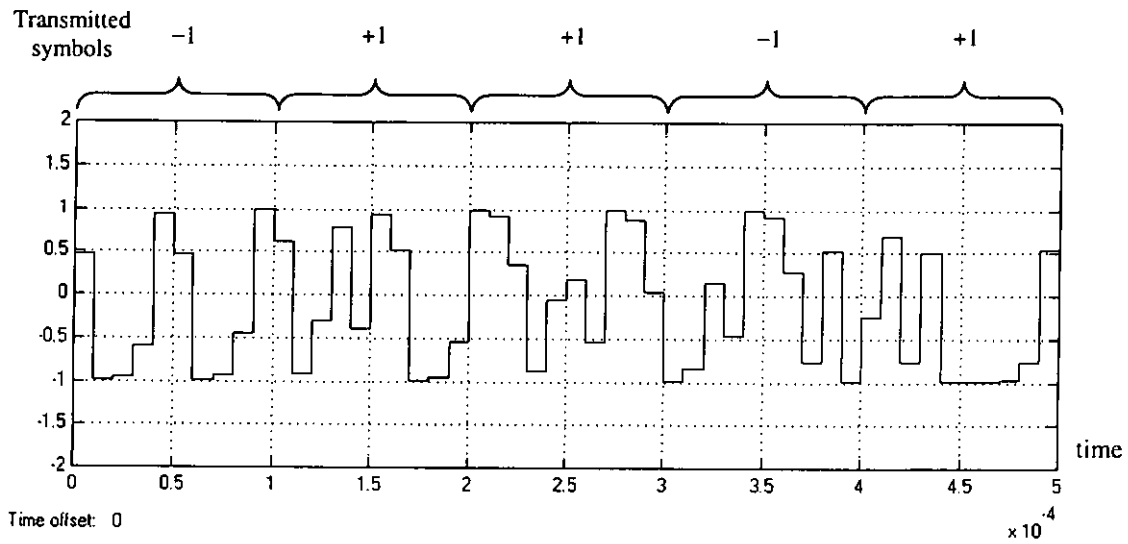


Figure 3-2(c) Transmitted waveform $s(t)$ of a CSK communications system

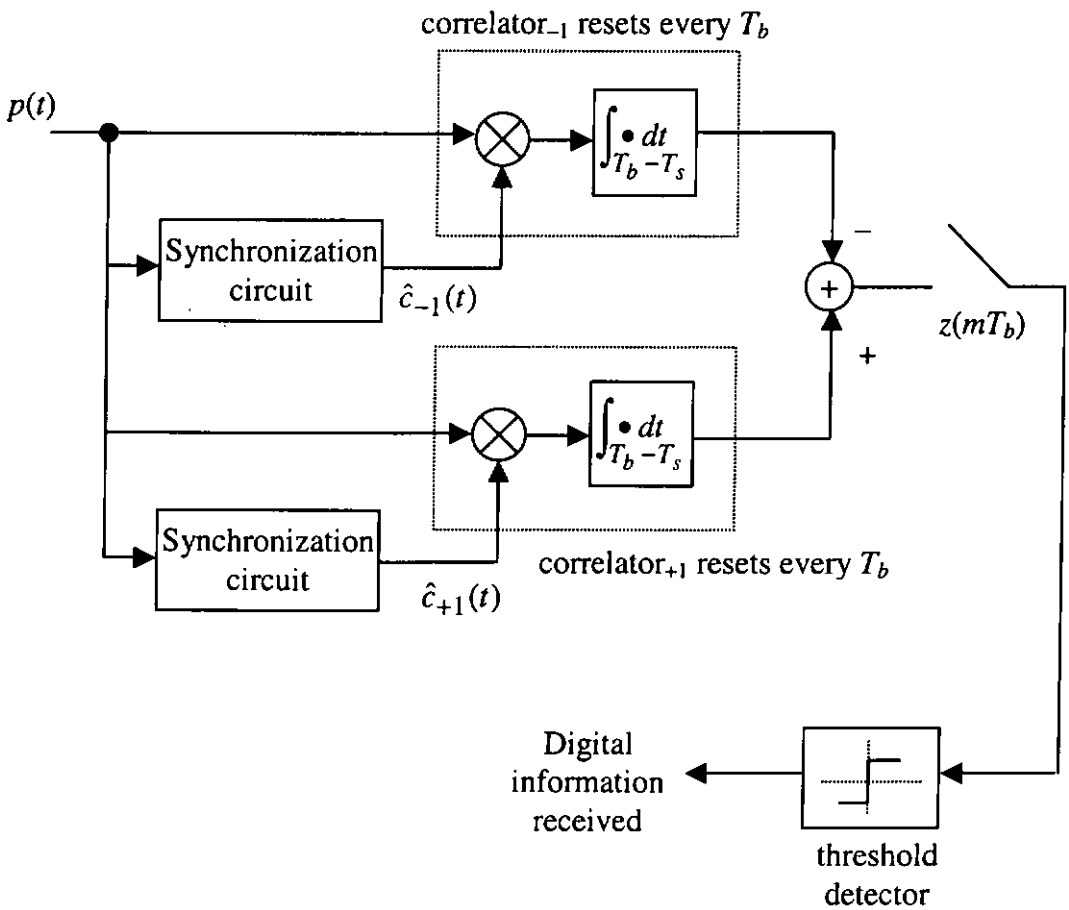


Figure 3-3 Coherent CSK demodulator

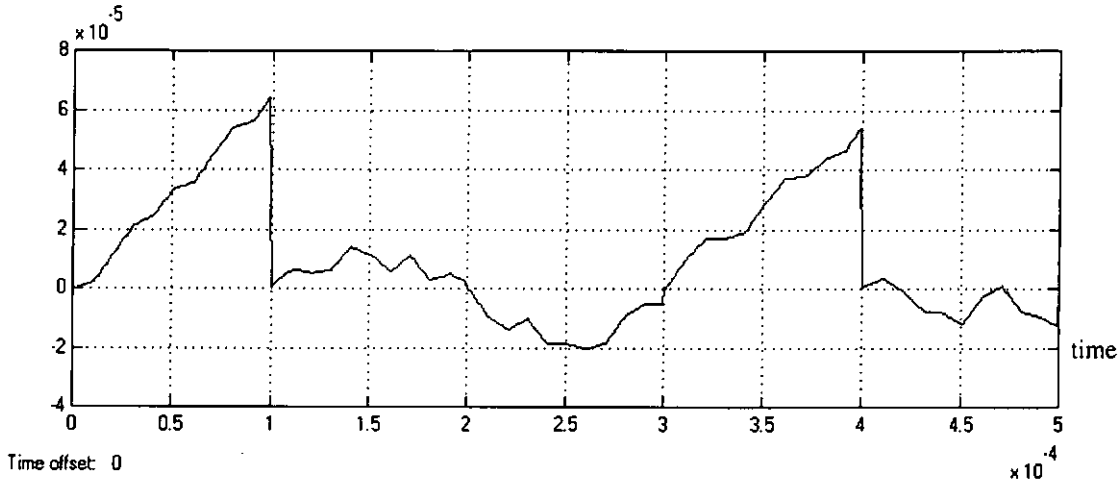


Figure 3-4(a) Output of correlator$_{-1}$ for large SNR

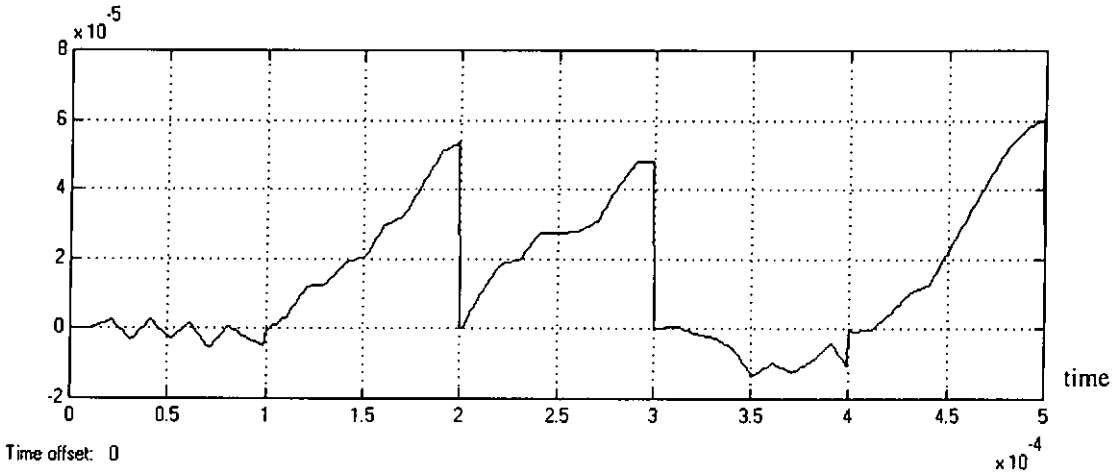


Figure 3-4(b) Output of correlator$_{+1}$ for large SNR

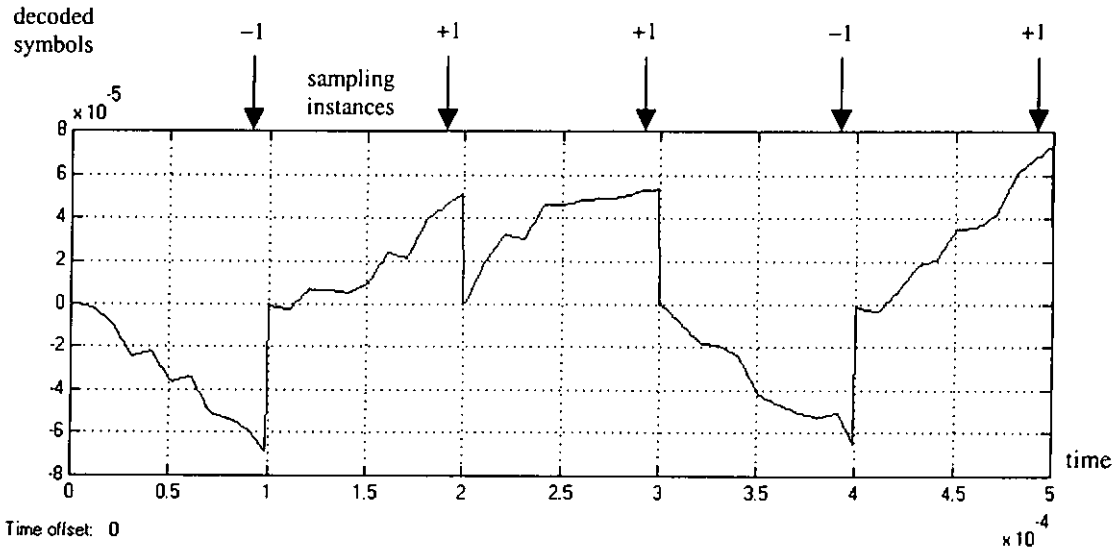


Figure 3-4(c) Output of the adder and the decoded symbols for large SNR

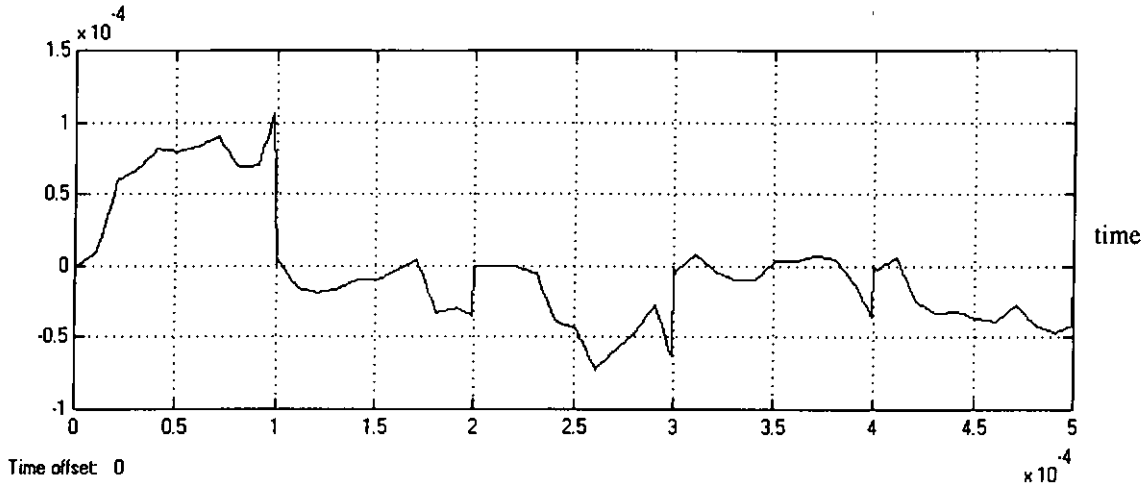


Figure 3-5(a) Output of correlator$_{-1}$ for small SNR

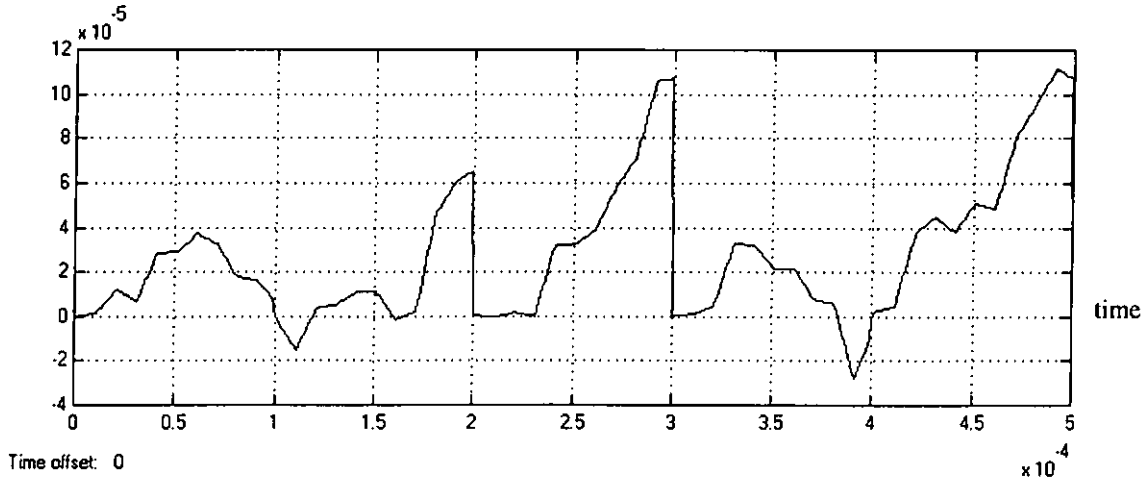


Figure 3-5(b) Output of correlator$_{+1}$ for small SNR

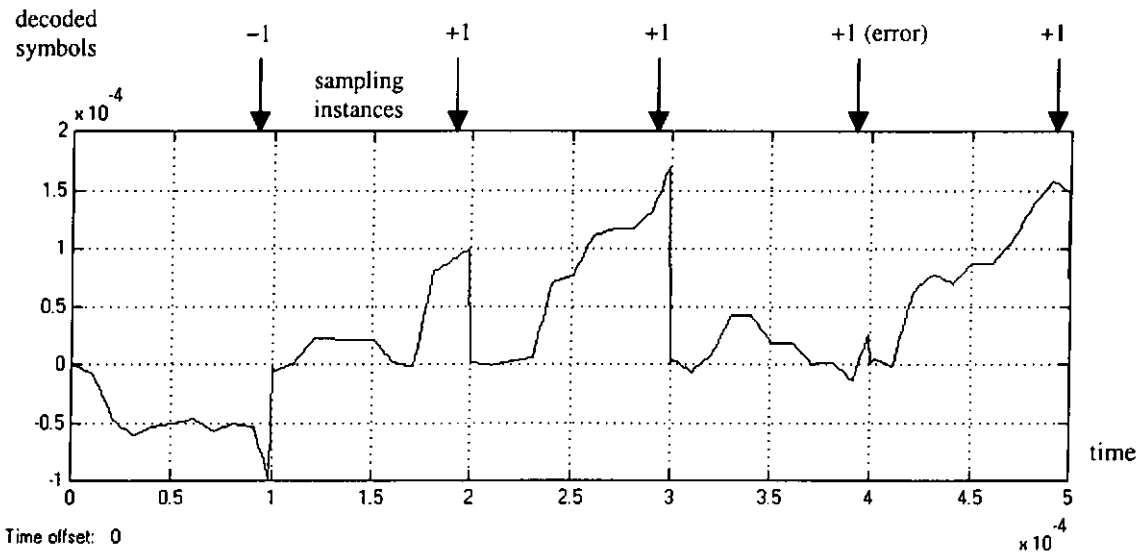


Figure 3-5(c) Output of the adder and the decoded symbols for small SNR

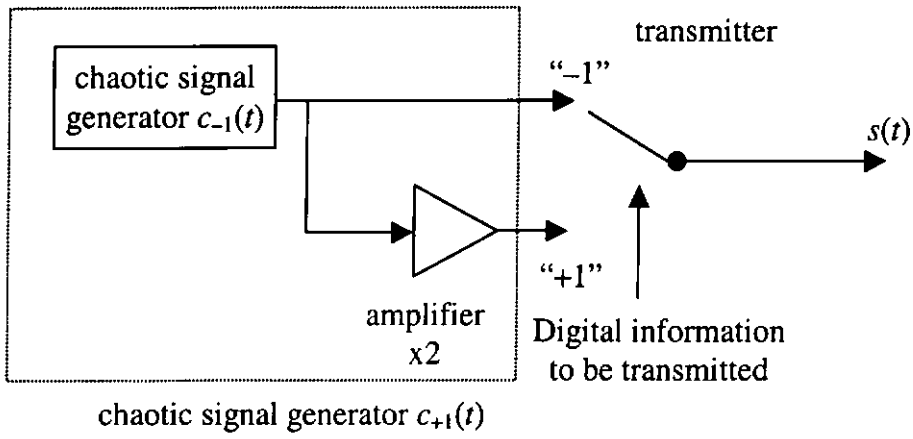


Figure 3-6 Chaos generators with different average bit energies used in a CSK transmitter

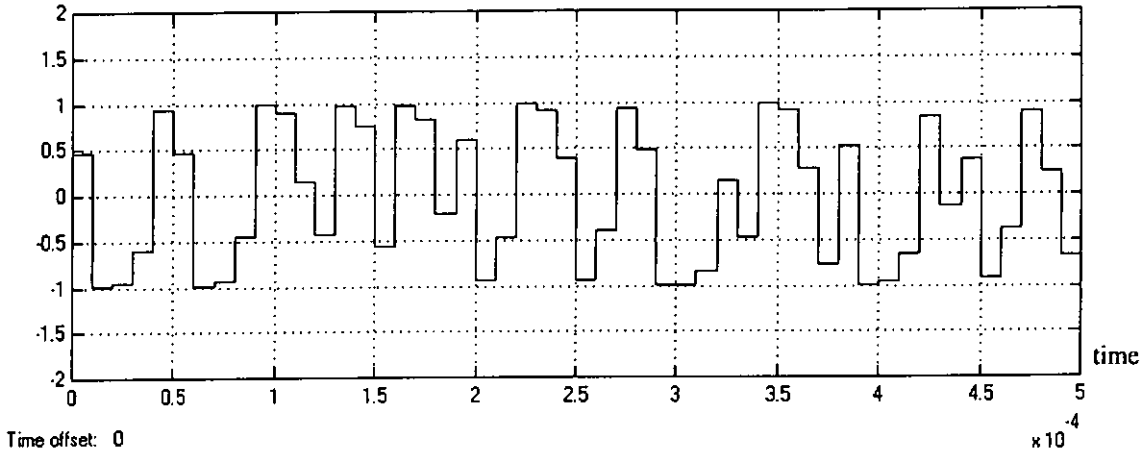


Figure 3-7(a) Basis function $c_{-1}(t)$ for noncoherent CSK detection

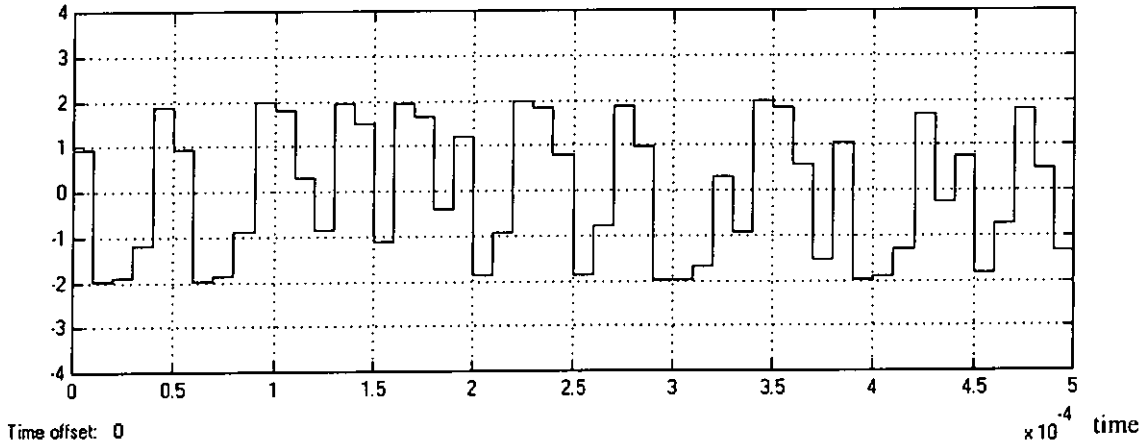


Figure 3-7(b) Basis function $c_{+1}(t)$ for noncoherent CSK detection

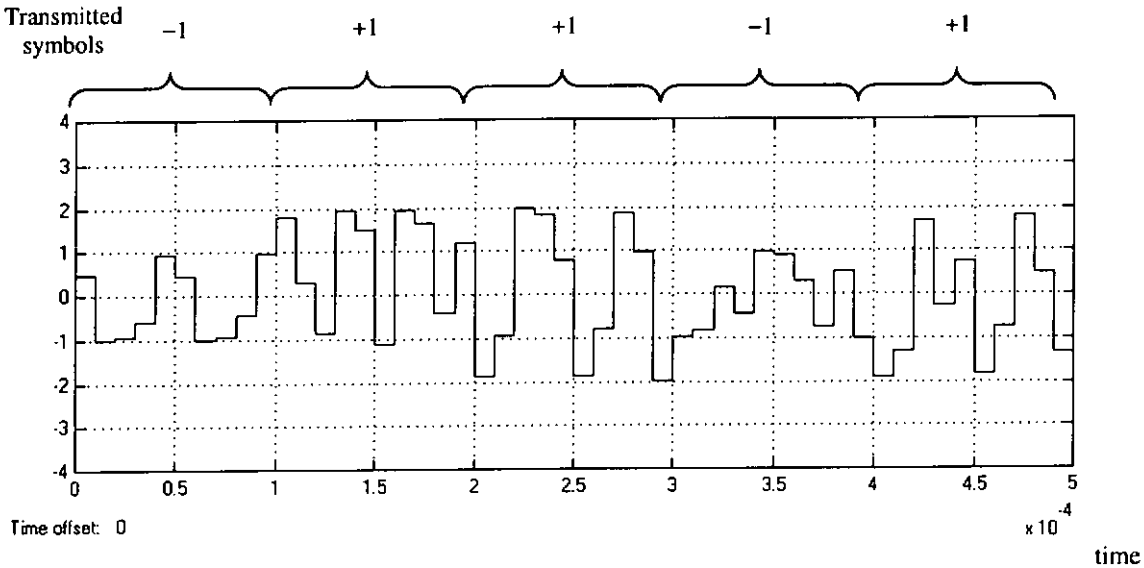


Figure 3-7(c) Transmitted waveform $s(t)$ for noncoherent CSK detection

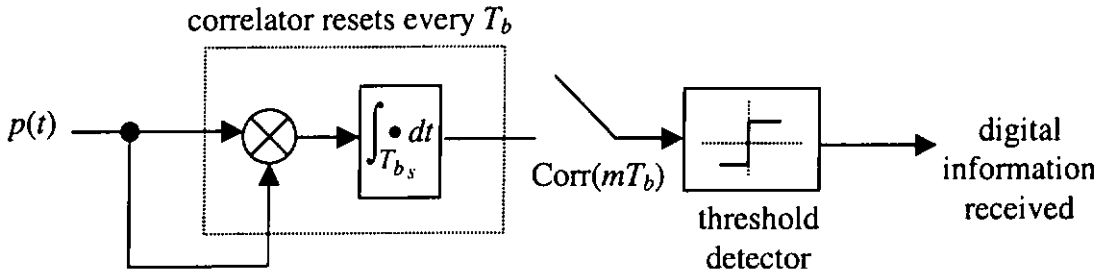


Figure 3-8 Noncoherent CSK demodulator

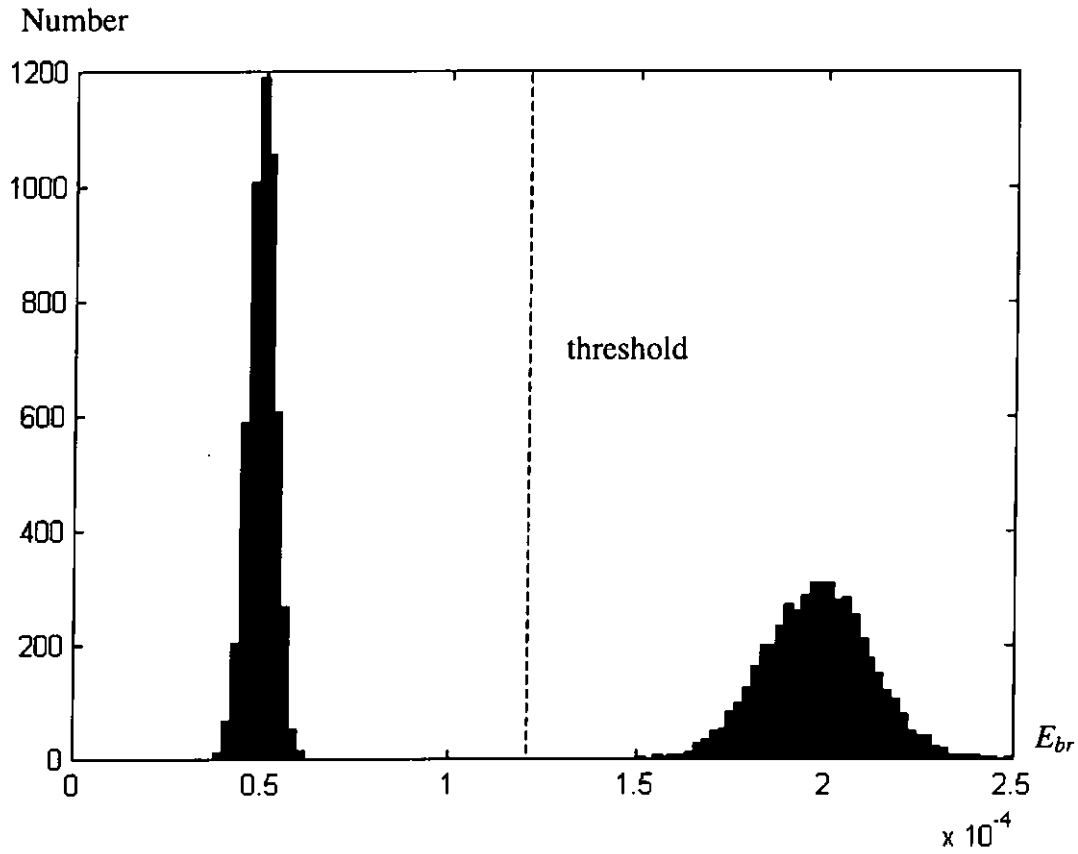


Figure 3-9 Histogram of received bit energy E_{br} for a noncoherent CSK receiver with $\overline{E_b} / N_0$ =81dB

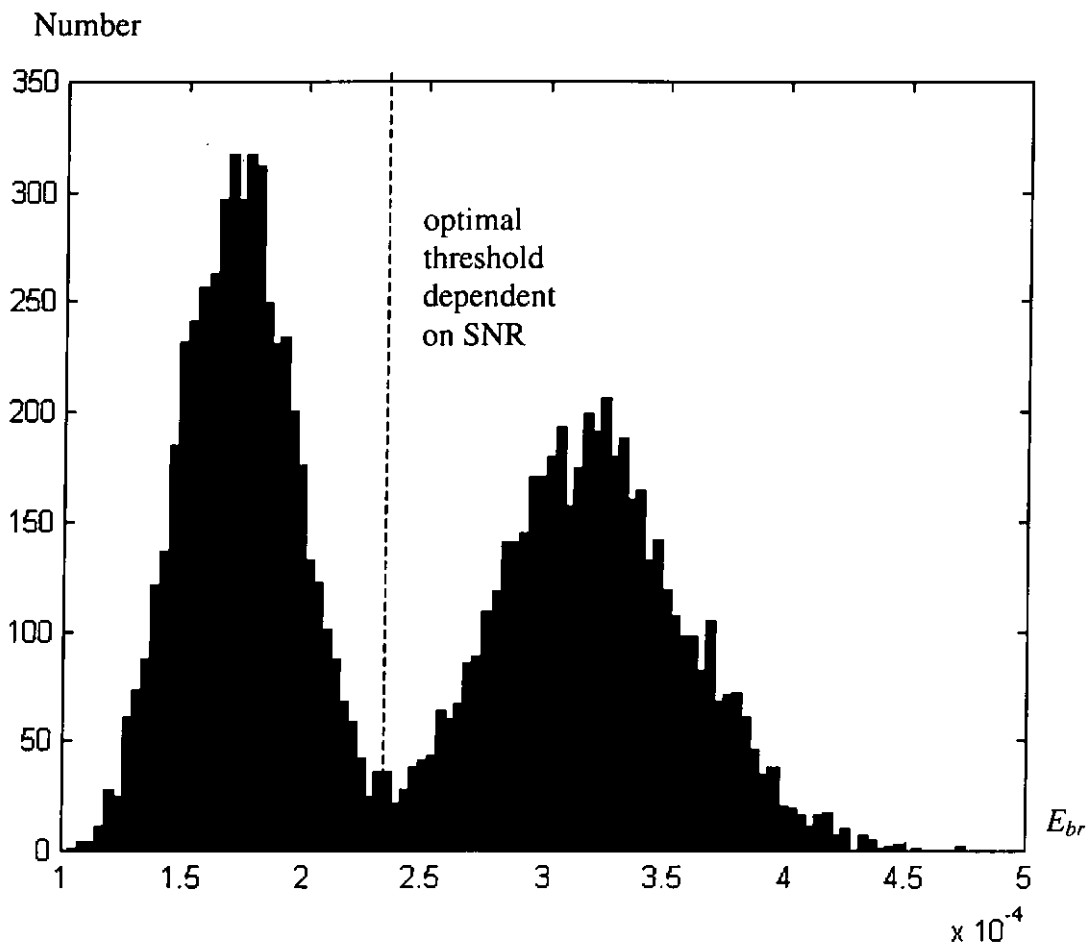


Figure 3-10 Histogram of received bit energy E_{br} for a noncoherent CSK receiver with $\overline{E_b} / N_0 = 17\text{dB}$

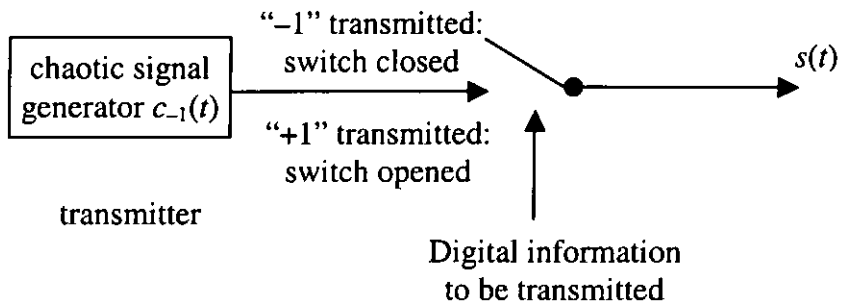


Figure 3-11 Chaotic on-off-keying transmitter

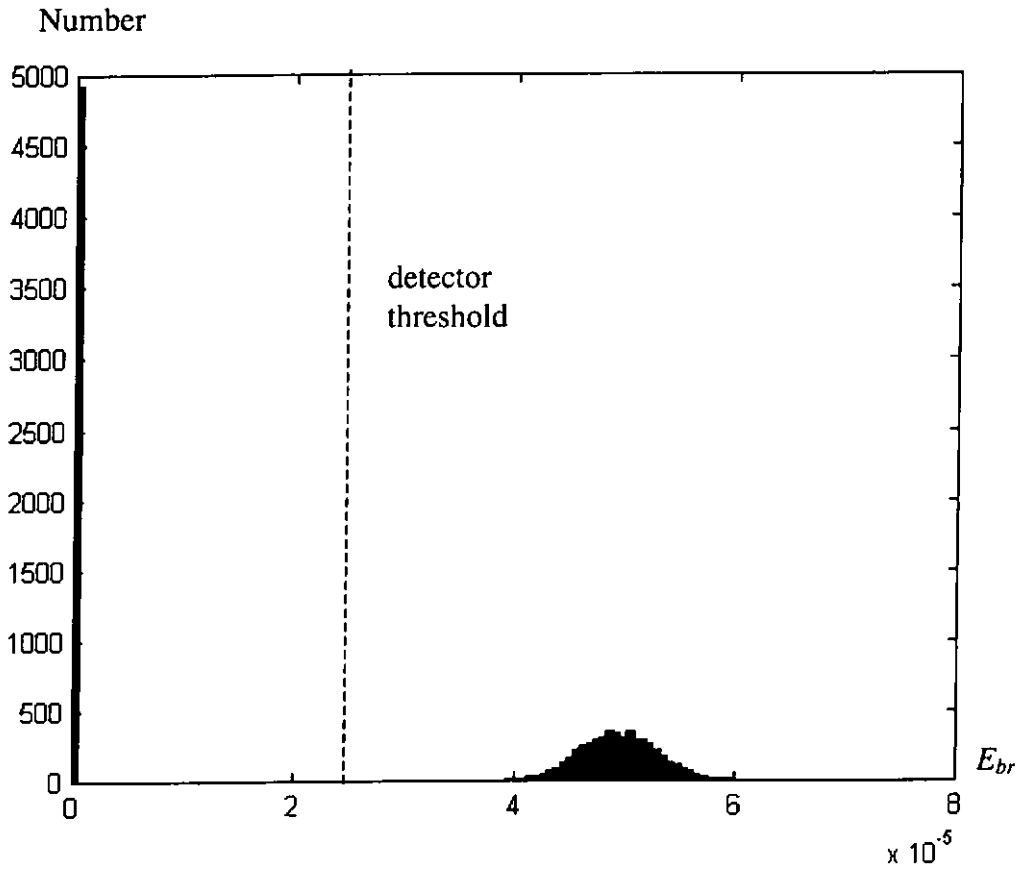


Figure 3-12 Histogram of received bit energy E_{br} for a COOK receiver under a noiseless environment

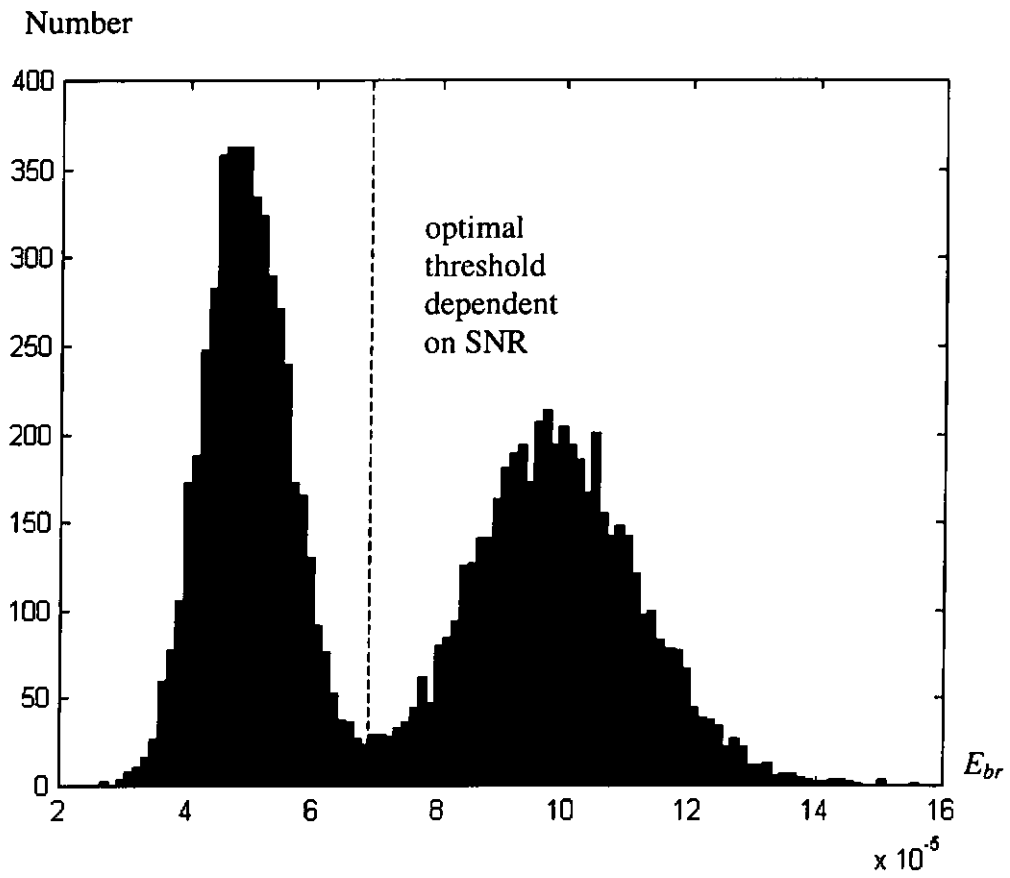


Figure 3-13 Histogram of received bit energy E_{br} for a COOK receiver with $\overline{E_b} / N_0$ =14dB

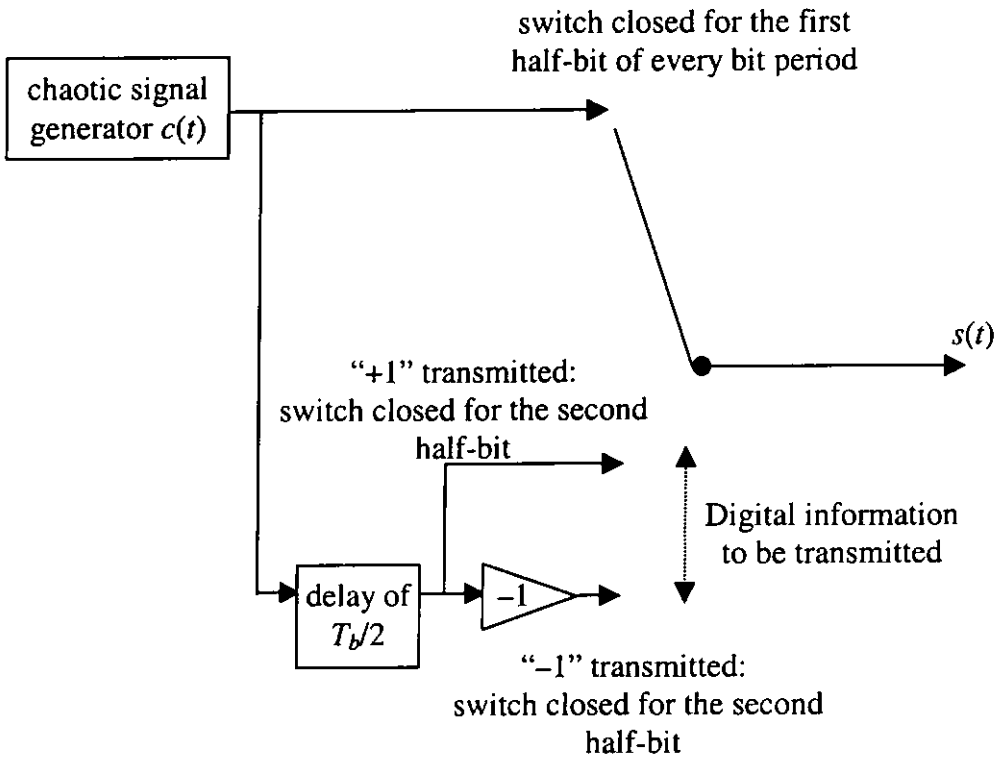


Figure 3-14 Transmitter of a DCSK modulator

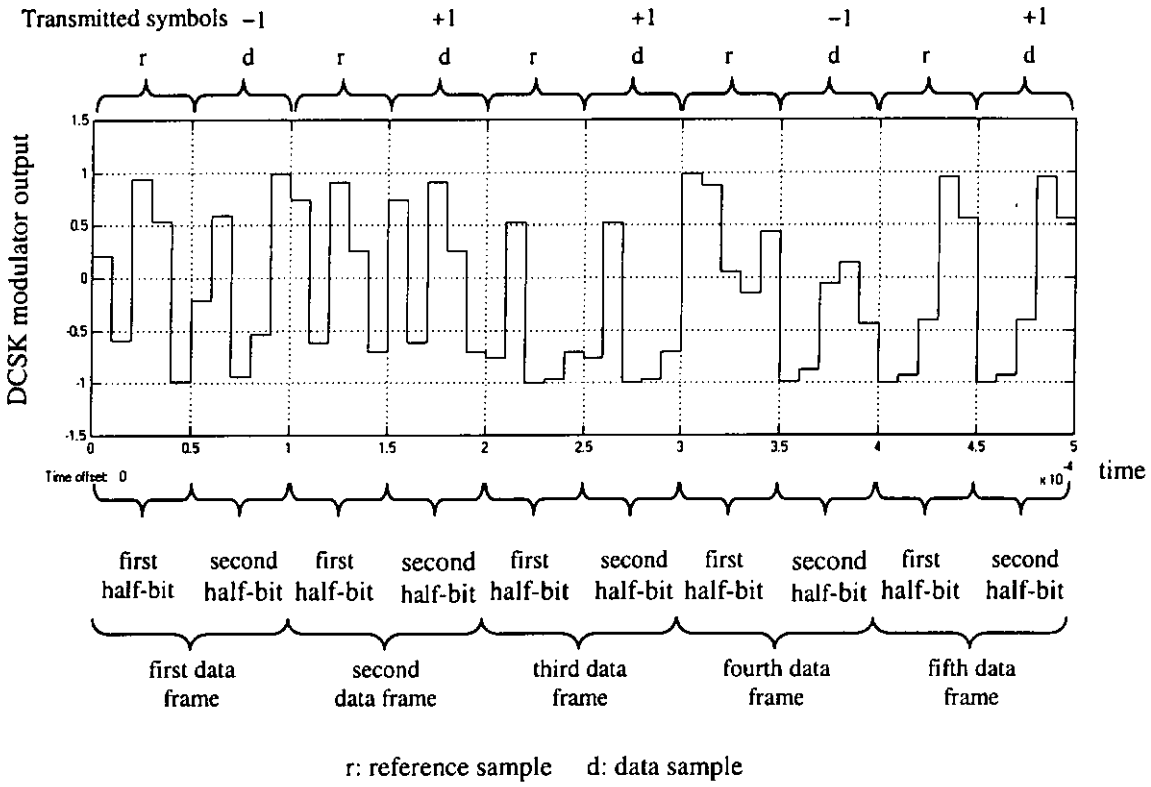


Figure 3-15 A typical DCSK signal

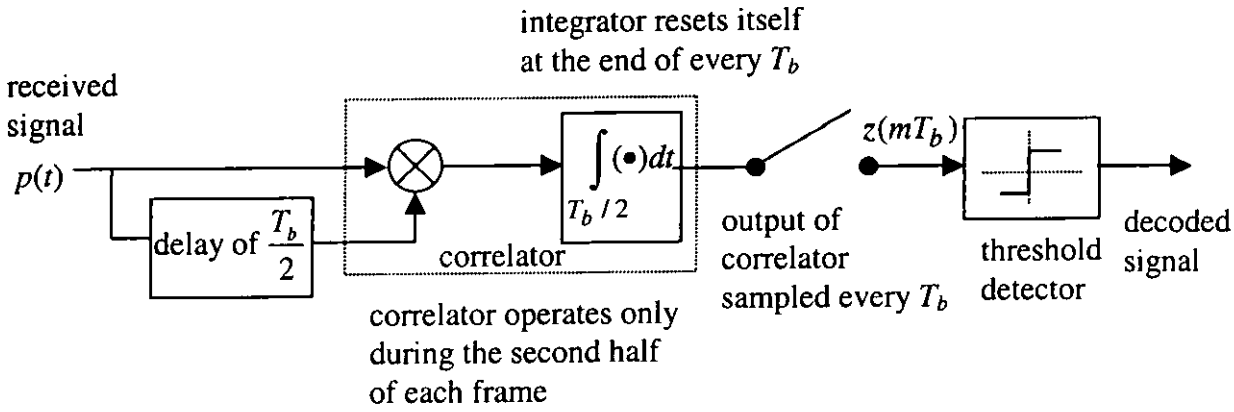


Figure 3-16 Block diagram of a DCSK correlator receiver

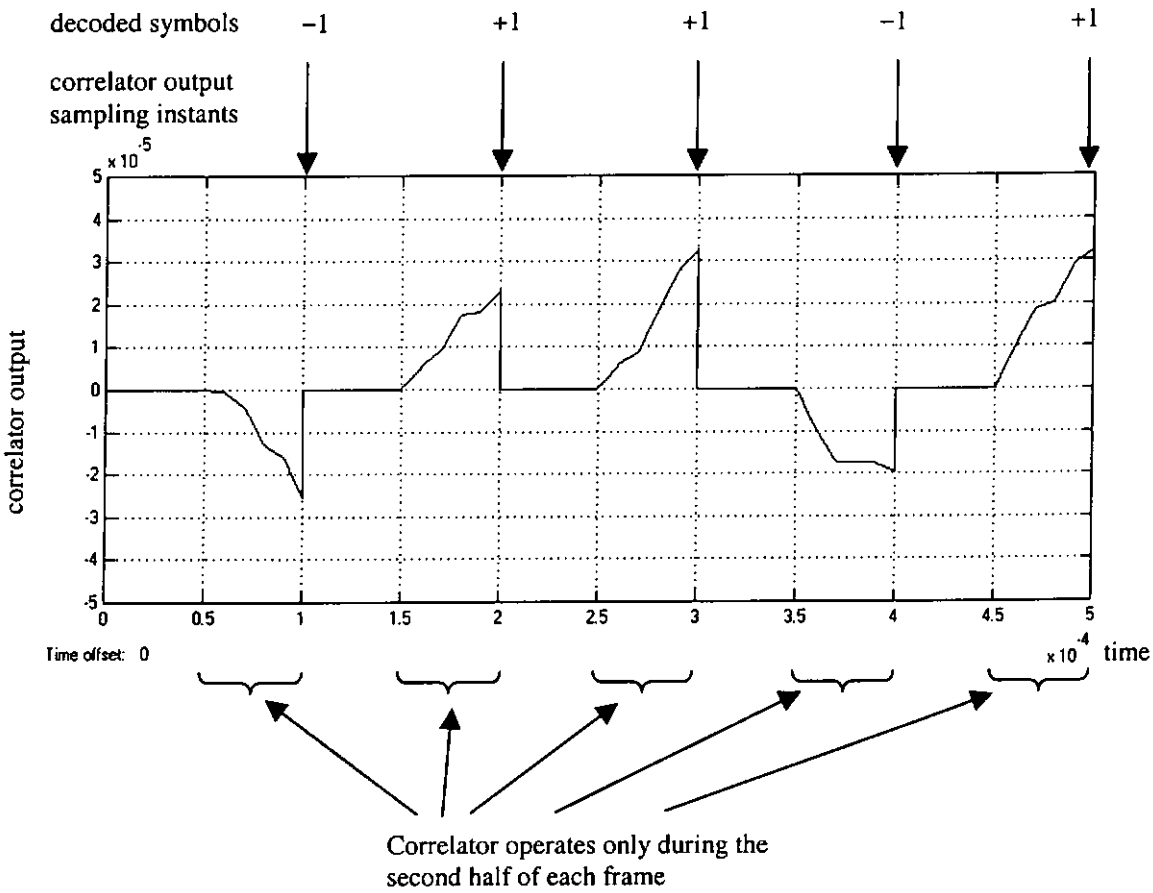


Figure 3-17 Output of the correlator and the decoded symbols in a DCSK correlator receiver

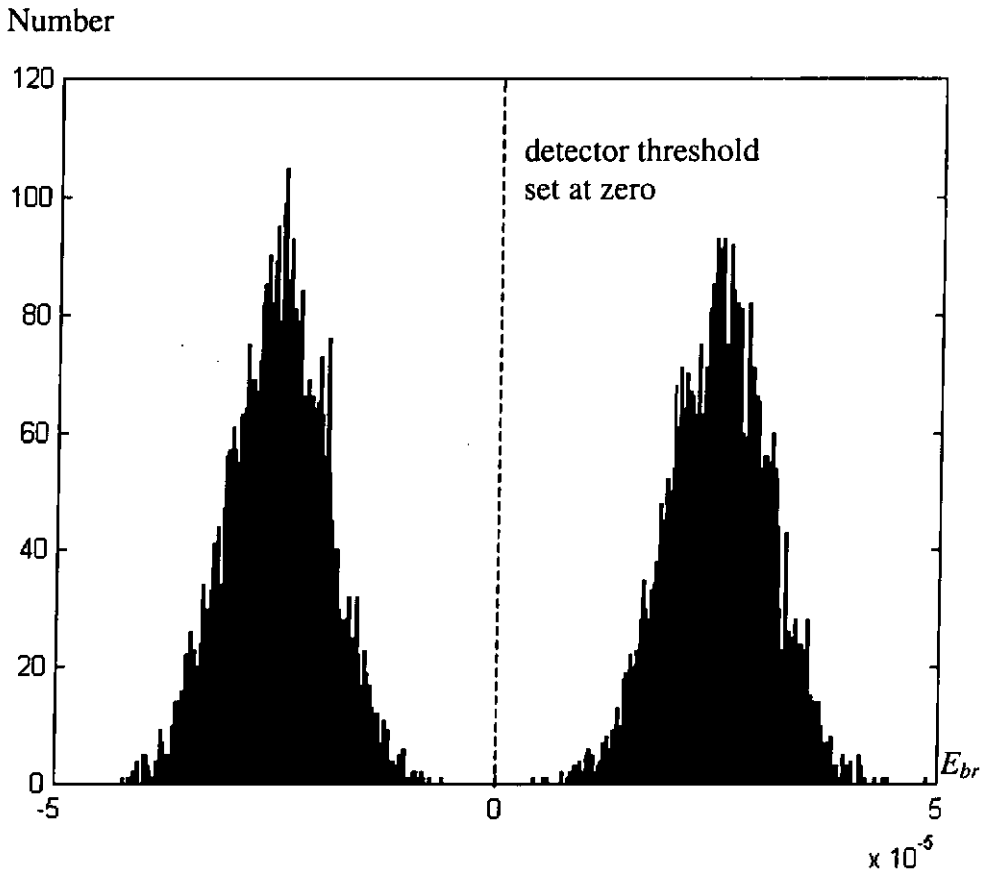


Figure 3-18 Histogram of correlator output for a DCSK receiver with $\overline{E_b} / N_0$ =170dB

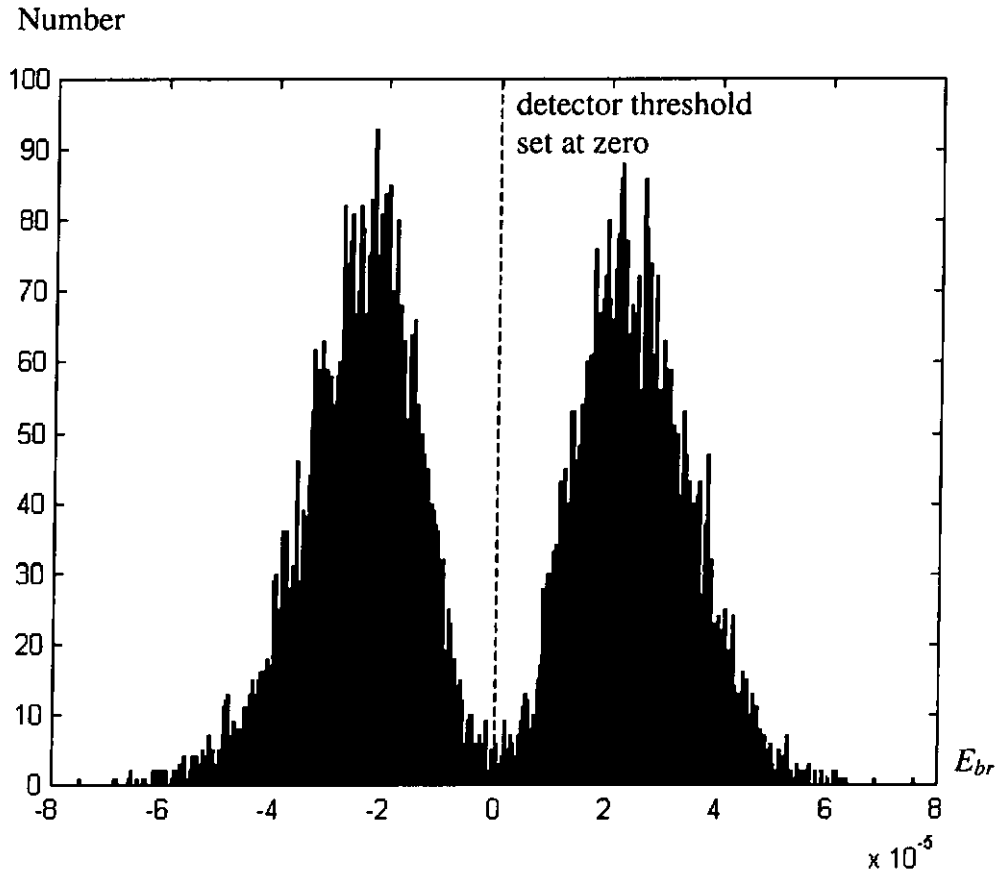


Figure 3-19 Histogram of correlator output for a DCSK receiver with $\overline{E_b} / N_0$ =13dB

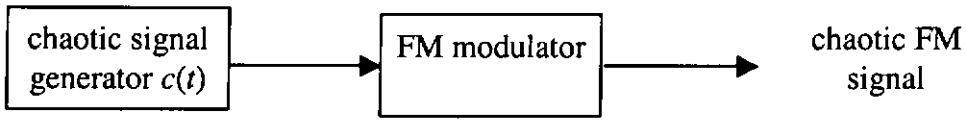


Figure 3-20 Chaotic FM generator

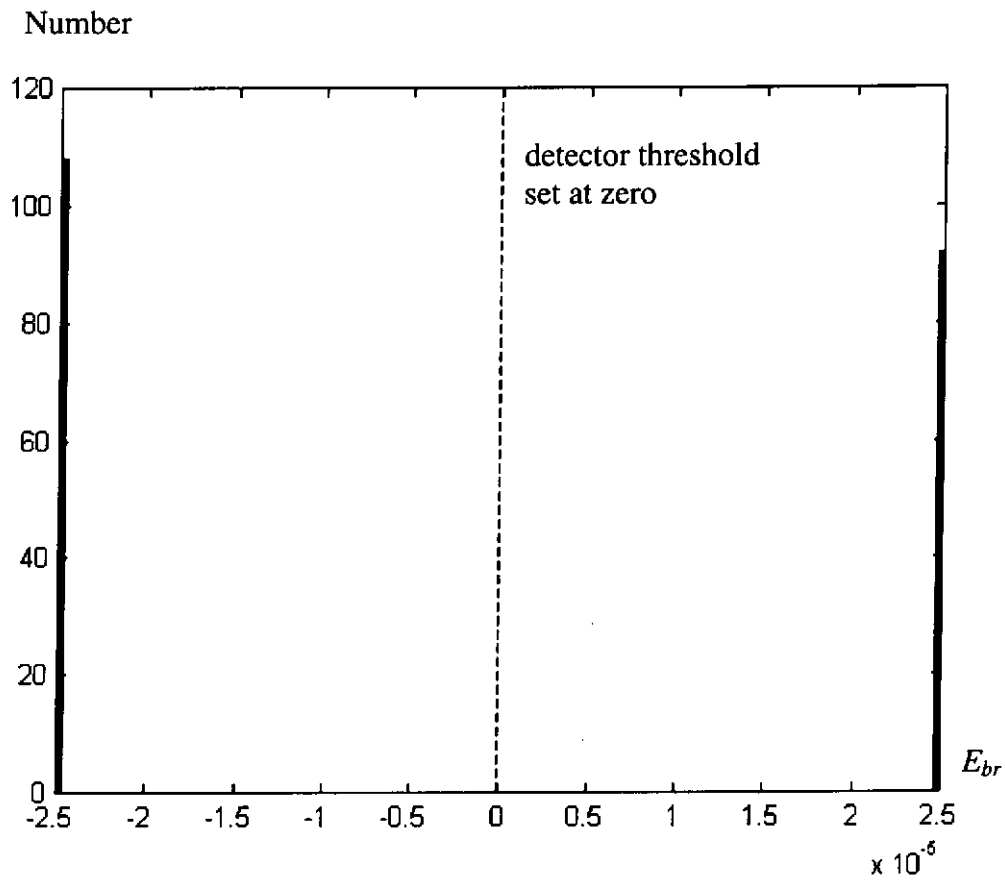


Figure 3-21 Histogram of correlator output for a FM-DCSK receiver under a noiseless environment

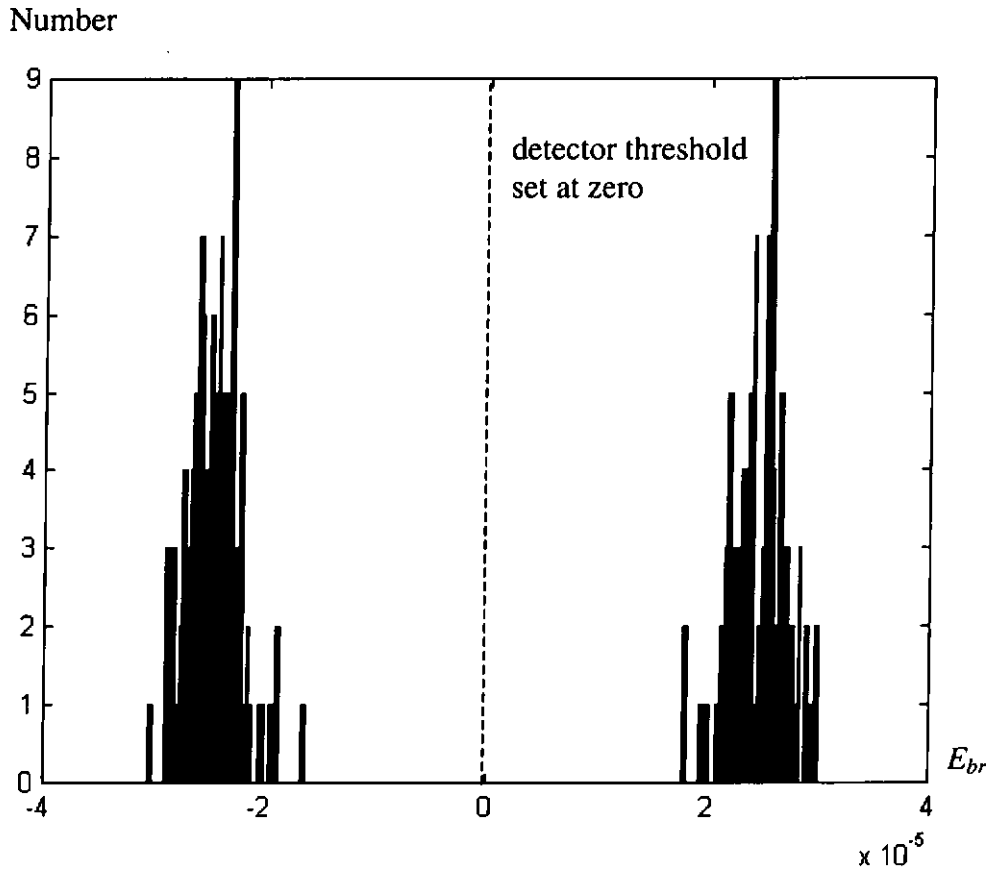


Figure 3-22 Histogram of correlator output for a FM-DCSK receiver with $\overline{E_b} / N_0 = 15\text{dB}$

CHAPTER 4

CHAOS SHIFT KEYING IN A MULTI-USER ENVIRONMENT

In the previous chapter, several digital modulation techniques based on chaos have been introduced. The basic structures of the transmitters and receivers, together with the modulation and demodulation methods, are also studied. In this chapter, we will investigate chaos shift keying (CSK) in more detail. The performances of a single-user coherent CSK system under noiseless and noisy environments will first be examined. Based on the cubic map described in Chapter 2, numerical bit error probabilities (BEPs) will be derived and simulations are performed to verify the numerical results.

In conventional communications systems, the allocated spectrum is shared by a number of users. Multiple access techniques such as frequency division multiple access (FDMA), time division multiple access (TDMA) and code division multiple access (CDMA) are commonly used. Since CSK spreads the spectrum of the data signal over a much larger bandwidth, multiple access becomes an essential feature for practical implementation of the system. Furthermore, it is imperative that more users are included in the same bandwidth without causing excessive interference to one another. Therefore, the coherent CSK system will also be evaluated under a multi-user environment. The architecture of such a system will be described. Numerical derivations of the BEPs

under noiseless/noisy conditions are shown again and compared with the simulation results. Finally, the results are compared with a conventional spread spectrum communications system using Gold code as the spreading code.

4.1 Single-User CSK Communications System

In this section, the performance of a single-user coherent CSK communications system under a noiseless/noisy condition is fully examined. The block diagram of a CSK communications system in Figure 3-1 is depicted in Figure 4-1 again. Assume that chaos is generated by the map $x_{\pm 1,n+1} = g(x_{\pm 1,n})$ but with different initial conditions. Moreover, the outputs of the chaotic signal generators are given by

$$c_{-1}(t) = \sum_{k=0}^{\infty} x_{-1,k}\, r(t - kT_c) \tag{4-1}$$

and $$c_{+1}(t) = \sum_{k=0}^{\infty} x_{+1,k}\, r(t - kT_c) \tag{4-2}$$

where $r(t)$ is a rectangular pulse of unit amplitude and width T_c, i.e.,

$$r(t) = \begin{cases} 1 & 0 \le t < T_c \\ 0 & \text{elsewhere.} \end{cases} \tag{4-3}$$

In CSK, if a binary "−1" is to be transmitted during the interval $[(m-1)T_b, mT_b)$, $c_{-1}(t)$ will be sent. On the other hand, if "+1" needs to be transmitted, $c_{+1}(t)$ is sent. Assume that the system starts at $t = 0$ and the binary data to be transmitted has a period of T_b. Denote the transmitted data by $\{d_1, d_2, d_3, ...\} \in \{-1, +1\}$. Let β be the spreading factor, defined as T_b/T_c, where β is an integer. Using the aforementioned arrangement, the transmitted waveform for the mth bit is given by

$$v^m(t) = \sum_{k=0}^{\beta-1} x_{d_m,k+(m-1)\beta} r[t-(kT_c+(m-1)T_b)] \tag{4-4}$$

The overall transmitted waveform is

$$s(t) = \sum_{m=1}^{\infty} v^m(t). \tag{4-5}$$

Figure 4-2 shows some typical waveforms of $c_{-1}(t)$, $c_{+1}(t)$ and $s(t)$ for a spreading factor of 10.

Assume that the only channel distortion is due to the noise source $n(t)$, which is an additive white Gaussian noise (AWGN) with a two sided power spectral density (psd) of

$$S_n(f) = \frac{N_0}{2} \text{ for all } f, \tag{4-6}$$

as in Figure 4-3. It can be shown that in our analyses that followed, $n(t)$ can be represented by an equivalent noise source $n'(t)$ (Appendix D) given by

$$n'(t) = \sum_{k=0}^{\infty} \xi_k r(t-kT_c) \tag{4-7}$$

where the coefficients ξ_k are independent Gaussian random variables with zero mean and variance

$$\sigma_{n'}^2 = \frac{N_0}{2T_c}. \tag{4-8}$$

As a consequence, the CSK communications system in Figure 4-1 is re-drawn in Figure 4-4. Figure 4-5 shows a coherent CSK demodulator where it is assumed that the synchronization circuits can reproduce the chaotic signals perfectly and the synchronization time is assumed to be negligible compared with the bit period. Assume that the chaotic signals are generated by the cubic map in Chapter 2, i.e.,

$$g(x_{n+1}) = 4x_n^3 - 3x_n\,, \tag{4-9}$$

but with different initial conditions. We can now derive the numerical bit error probabilities.

4.1.1 Numerical Bit Error Probability

The input to the demodulator is given by

$$\begin{aligned} p'(t) &= s(t) + n'(t) \\ &= \sum_{m=1}^{\infty} v^m(t) + \sum_{k=0}^{\infty} \xi_k r(t - kT_c) \\ &= \sum_{m=1}^{\infty}\sum_{k=0}^{\beta-1} x_{d_m,k+(m-1)\beta}\, r[t - (kT_c + (m-1)T_b)] + \sum_{k=0}^{\infty} \xi_k r(t - kT_c). \end{aligned} \tag{4-10}$$

For the mth received symbol, the output of the correlator$_{-1}$ at the end of the period is given by

$$\begin{aligned} \mathrm{Corr}_{-1}(mT_b) &= \int_{(m-1)T_b}^{mT_b} p'(t)c_{-1}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} [v^m(t) + \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k r(t - kT_c)]c_{-1}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} \left[\sum_{k=0}^{\beta-1} x_{d_m,k+(m-1)\beta}\, r[t - (kT_c + (m-1)T_b)] + \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k r(t - kT_c)\right] c_{-1}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} \left[\sum_{k=(m-1)\beta}^{m\beta-1} x_{d_m,k} r(t - kT_c) + \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k r(t - kT_c)\right]\left[\sum_{k=(m-1)\beta}^{m\beta-1} x_{-1,k} r(t - kT_c)\right] dt. \end{aligned}$$

Therefore,

$$\mathrm{Corr}_{-1}(mT_b) = T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{d_m,k} x_{-1,k} + \xi_k x_{-1,k}]\ . \tag{4-11}$$

Similarly, the output of the correlator$_{+1}$ can be shown equal to

$$\mathrm{Corr}_{+1}(mT_b) = T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{d_m,k} x_{+1,k} + \xi_k x_{+1,k}]. \tag{4-12}$$

The output of the adder, i.e., the input to the threshold detector, at this time instant is

$$\begin{aligned} z(mT_b) &= \mathrm{Corr}_{+1}(mT_b) - \mathrm{Corr}_{-1}(mT_b) \\ &= T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{d_m,k} x_{+1,k} + \xi_k x_{+1,k} - x_{d_m,k} x_{-1,k} - \xi_k x_{-1,k}]. \end{aligned} \tag{4-13}$$

Suppose a "+1" has been transmitted for the mth symbol, i.e., $d_m = +1$, the input of the detector will be given by

$$\begin{aligned} z_{+1}(mT_b) &= T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{+1,k} x_{+1,k} + \xi_k x_{+1,k} - x_{+1,k} x_{-1,k} - \xi_k x_{-1,k}] \\ &= T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{+1,k}^2 + \xi_k x_{+1,k} - x_{+1,k} x_{-1,k} - \xi_k x_{-1,k}]. \end{aligned} \tag{4-14}$$

Similarly, if a "−1" is transmitted,

$$\begin{aligned} z_{-1}(mT_b) &= T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{-1,k} x_{+1,k} + \xi_k x_{+1,k} - x_{-1,k} x_{-1,k} - \xi_k x_{-1,k}] \\ &= T_c \sum_{k=(m-1)\beta}^{m\beta-1} [x_{-1,k} x_{+1,k} + \xi_k x_{+1,k} - x_{-1,k}^2 - \xi_k x_{-1,k}]. \end{aligned} \tag{4-15}$$

Using the notations defined in Section 2.3.4, equation (4-14) is expressed as

$$\begin{aligned} z_{+1}(mT_b) = \beta T_c [&\gamma_{x_{+1}}((m-1)\beta,(m-1)\beta,\beta) + \gamma_{x_{+1}\xi}((m-1)\beta,(m-1)\beta,\beta) \\ &- \gamma_{x_{+1}x_{-1}}((m-1)\beta,(m-1)\beta,\beta) - \gamma_{x_{-1}\xi}((m-1)\beta,(m-1)\beta,\beta)]. \end{aligned} \tag{4-16}$$

As shown in Section 2.3.4, each of the four terms in equation (4-16) can be modelled as a normal random variable. Assume that the random variables are independent of each other. $z_{+1}(mT_b)$ will also be normally distributed [Ross 93] with mean

$$\overline{z_{+1}(mT_b)} = \beta T_c[\overline{\gamma_{x_{+1}}((m-1)\beta,(m-1)\beta,\beta)} + \overline{\gamma_{x_{+1}\xi}((m-1)\beta,(m-1)\beta,\beta)} - \overline{\gamma_{x_{+1}x_{-1}}((m-1)\beta,(m-1)\beta,\beta)} - \overline{\gamma_{x_{-1}\xi}((m-1)\beta,(m-1)\beta,\beta)}] \tag{4-17}$$

and variance

$$\begin{aligned}\mathrm{var}[z_{+1}(mT_b)] = (\beta T_c)^2\{&\mathrm{var}[\gamma_{x_{+1}}((m-1)\beta,(m-1)\beta,\beta)] + \mathrm{var}[\gamma_{x_{+1}\xi}((m-1)\beta,(m-1)\beta,\beta)] \\ &+ \mathrm{var}[\gamma_{x_{+1}x_{-1}}((m-1)\beta,(m-1)\beta,\beta)] + \mathrm{var}[\gamma_{x_{-1}\xi}((m-1)\beta,(m-1)\beta,\beta)]\}\end{aligned} \tag{4-18}$$

where var[U] represents the variance of U.

If $z_{+1}(mT_b)$ is larger than zero, a "+1" is decoded for the mth symbol. Otherwise, a "−1" is detected. The error probability given a "+1" has been transmitted is given by (Appendix E)

$$\mathrm{Prob}(z_{+1}(mT_b) < 0 \,|\, \text{"+1" is transmitted}) = Q\left(\frac{\overline{z_{+1}(mT_b)}}{\sqrt{\mathrm{var}[z_{+1}(mT_b)]}}\right) \tag{4-19}$$

where the Q-function in (4-19) [Proa 94] is defined as

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp(\frac{-t^2}{2})dt. \tag{4-20}$$

Using the results in Table 2-2, which is repeated in Table 4-1, the values of $\overline{z_{+1}(mT_b)}$ and $\mathrm{var}[z_{+1}(mT_b)]$ can now be found.

For β=100,

$$\begin{aligned}\overline{z_{+1}(mT_b)} &= \beta T_c[0.5+0-0-0] \\ &= 0.5\beta T_c\end{aligned} \tag{4-21}$$

and

$$\begin{aligned}\mathrm{var}[z_{+1}(mT_b)] &= (\beta T_c)^2[1.24\mathrm{x}10^{-3} + 5.0\mathrm{x}10^{-3}\sigma_{n'}^2 + 2.5\mathrm{x}10^{-3} + 5.0\mathrm{x}10^{-3}\sigma_{n'}^2] \\ &= (\beta T_c)^2[3.74\mathrm{x}10^{-3} + 1.0\mathrm{x}10^{-2}\sigma_{n'}^2] \\ &= (\beta T_c)^2\left[3.74\mathrm{x}10^{-3} + 1.0\mathrm{x}10^{-2}\frac{N_0}{2T_c}\right].\end{aligned} \tag{4-22}$$

For $\beta = 1000$,

$$\begin{aligned}\overline{z_{+1}(mT_b)} &= \beta T_c[0.5+0-0-0] \\ &= 0.5\beta T_c\end{aligned} \tag{4-23}$$

and

$$\begin{aligned}\mathrm{var}[z_{+1}(mT_b)] &= (\beta T_c)^2[1.24\mathrm{x}10^{-4} + 5.0\mathrm{x}10^{-4}\sigma_{n'}^2 + 2.5\mathrm{x}10^{-4} + 5.0\mathrm{x}10^{-4}\sigma_{n'}^2] \\ &= (\beta T_c)^2\left[3.74\mathrm{x}10^{-4} + 1.0\mathrm{x}10^{-3}\frac{N_0}{2T_c}\right].\end{aligned} \tag{4-24}$$

Hence,

$$\mathrm{Prob}(z_{+1}(mT_b) < 0 \,|\, \text{"+1" is transmitted}) = \begin{cases} Q\left(\dfrac{0.5}{\sqrt{3.74\mathrm{x}10^{-3} + 1.0\mathrm{x}10^{-2} N_0 / 2T_c}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{3.74\mathrm{x}10^{-4} + 1.0\mathrm{x}10^{-3} N_0 / 2T_c}}\right) & \beta = 1000. \end{cases} \tag{4-25}$$

Using the same procedures, it can be shown that if a "–1" is transmitted,

$$\overline{z_{-1}(mT_b)} = -0.5\beta T_c \quad \text{for } \beta = 100 \text{ or } 1000, \tag{4-26}$$

$$\mathrm{var}[z_{-1}(mT_b)] = \begin{cases} (\beta T_c)^2\left[3.74\mathrm{x}10^{-3} + 1.0\mathrm{x}10^{-2}\dfrac{N_0}{2T_c}\right] & \beta = 100 \\ (\beta T_c)^2\left[3.74\mathrm{x}10^{-4} + 1.0\mathrm{x}10^{-3}\dfrac{N_0}{2T_c}\right] & \beta = 1000 \end{cases} \tag{4-27}$$

and

$$\mathrm{Prob}(z_{-1}(mT_b) > 0 \,|\, \text{"−1" is transmitted}) = \begin{cases} Q\left(\dfrac{0.5}{\sqrt{3.74\mathrm{x}10^{-3} + 1.0\mathrm{x}10^{-2} N_0 / 2T_c}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{3.74\mathrm{x}10^{-4} + 1.0\mathrm{x}10^{-3} N_0 / 2T_c}}\right) & \beta = 1000. \end{cases} \tag{4-28}$$

By making use of equations (4-25) and (4-28), the overall bit error probability of a single-user coherent CSK system under AWGN is derived below.

$$\mathrm{BEP}_{1\text{-user}} = \mathrm{Prob}(z_{+1}(mT_b) < 0 \mid \text{“+1” is transmitted})P^{+}$$

$$+ \mathrm{Prob}(z_{-1}(mT_b) > 0 \mid \text{“−1” is transmitted})P^{-}$$

$$= \begin{cases} Q\left(\dfrac{0.5}{\sqrt{3.74\mathrm{x}10^{-3} + 1.0\mathrm{x}10^{-2} N_0 / 2T_c}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{3.74\mathrm{x}10^{-4} + 1.0\mathrm{x}10^{-3} N_0 / 2T_c}}\right) & \beta = 1000 \end{cases} \tag{4-29}$$

where P^{+} is the probability of a “+1” being transmitted and P^{-} is the probability of a “−1” being transmitted. Note that $P^{+} + P^{-} = 1$.

Define the average bit energy of the system as

$$\overline{E_b} = T_b \lim_{T\to\infty} [\frac{1}{T}\int_0^T s^2(t)dt]. \tag{4-30}$$

Applying equation (4-4), the average bit energy can be derived as below.

$$\begin{aligned}
\overline{E_b} &= T_b \lim_{T\to\infty}\left[\frac{1}{T}\int_0^T\left(\sum_{m=1}^{\infty} v^m(t)\right)^2 dt\right] \\
&= T_b \lim_{M\to\infty}\left[\frac{1}{MT_b}\int_0^{MT_b}\sum_{m=1}^{M}[v^m(t)]^2 dt\right] \\
&= T_b \lim_{M\to\infty}\left\{\frac{1}{MT_b}\sum_{m=1}^{M}\int_{(m-1)T_b}^{mT_b}\left[\sum_{k=0}^{\beta-1} x_{d_m,k+(m-1)\beta}\, r[t-(kT_c+(m-1)T_b)]\right]^2 dt\right\} \\
&= T_b \lim_{M\to\infty}\left[\frac{1}{MT_b}\sum_{m=1}^{M}\sum_{k=0}^{\beta-1} x^2_{d_m,k+(m-1)\beta} T_c\right] \\
&= T_c[\beta\overline{\gamma_{x_{+1}}(\kappa,\kappa,\beta)}P^{+} + \beta\overline{\gamma_{x_{-1}}(\kappa,\kappa,\beta)}P^{-}]
\end{aligned} \tag{4-31}$$

where $\gamma_{x+1}(\kappa,\kappa,\beta)$ and $\gamma_{x-1}(\kappa,\kappa,\beta)$ denote the mean-squared values of the chaotic sequence samples of length β taken from the chaotic series $\{x_{+1,n}\}$ and $\{x_{-1,n}\}$ respectively. Since both series are generated from the same map with different initial conditions, $\overline{\gamma_{x+1}(\kappa,\kappa,\beta)} = \overline{\gamma_{x-1}(\kappa,\kappa,\beta)} \equiv \overline{\gamma_x(\kappa,\kappa,\beta)}$. Equation (4-31) can be simplified to

$$\begin{aligned}\overline{E_b} &= T_c\beta\overline{\gamma_x(\kappa,\kappa,\beta)}[P^+ + P^-] \\ &= T_c\beta\overline{\gamma_x(\kappa,\kappa,\beta)} \\ &= 0.5T_c\beta \\ &= 0.5T_b\end{aligned} \tag{4-32}$$

for β = 100 or 1000. Using $T_b = \beta T_c$ and equation (4-32), equation (4-29) can also be expressed as

$$\begin{aligned}\mathrm{BEP}_{\text{1-user}} &= \begin{cases} Q\left(\dfrac{0.5}{\sqrt{3.74\text{x}10^{-3} + 1.0\text{x}10^{-2}\beta N_0 / 2T_b}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{3.74\text{x}10^{-4} + 1.0\text{x}10^{-3}\beta N_0 / 2T_b}}\right) & \beta = 1000 \end{cases} \\ &= \begin{cases} Q\left(\dfrac{\overline{E_b}}{\sqrt{3.74\text{x}10^{-3}T_b^2 + 0.5T_b N_0}}\right) & \beta = 100 \\ Q\left(\dfrac{\overline{E_b}}{\sqrt{3.74\text{x}10^{-4}T_b^2 + 0.5T_b N_0}}\right) & \beta = 1000. \end{cases}\end{aligned} \tag{4-33}$$

Assume that T_b=10^{-4}s. For a range of $\overline{E_b} / N_0$ values, the BEPs are computed using equation (4-33) and tabulated in Table 4-2. As expected, the BEPs decreases with increasing $\overline{E_b} / N_0$. Moreover, for the same $\overline{E_b} / N_0$, the BEP for β = 100 is worse than that for β = 1000. As can be judged from the aforementioned analysis, it is because of

the smaller variances in the auto- and cross-correlation values when β increases from 100 to 1000.

4.1.2 Simulations

Computer simulations have been performed based on the system model in Figure 4-4 and the demodulator in Figure 4-5. The bit period is assumed to be 10^{-4} s and β = 100 and 1000. For each of the different $\overline{E_b}/N_0$ values simulated, 10,000 bits have been transmitted and the BEPs are tabulated in Table 4-3.

4.1.3 Comparisons

The numerical and simulated BEPs are plotted against $\overline{E_b}/N_0$ in Figure 4-6. It can be observed that the results are very consistent. Next, we extend our analysis to a multi-user system.

4.2 Multi-User CSK Communications System

In the previous section, the performance of a single-user coherent CSK communications system under a noiseless/noisy condition has been fully examined. A coherent CSK communications system that can support multiple access is now evaluated. The equivalent models in Figures 4-4 and 4-5 will still be used.

Assume that there are N users within the system. The transmitter for the ith user is shown in Figure 4-7. The pair of chaotic series for user i is denoted by $\{x_{\pm i,n}\}$ and it is

assumed that all series are generated by the same map $x_{\pm i,n+1} = g(x_{\pm i,n})$ but with different initial conditions, where $g(x)$ is as defined in equation (4-9). Using similar notations as in the previous section, the outputs of the chaotic signal generators for user i are given by

$$c_{-i}(t) = \sum_{k=0}^{\infty} x_{-i,k} r(t - kT_c) \tag{4-34}$$

and $$c_{+i}(t) = \sum_{k=0}^{\infty} x_{+i,k} r(t - kT_c). \tag{4-35}$$

Denote the transmitted data for user i by $\{d_{i,1}, d_{i,2}, d_{i,3}, ...\} \in \{-1, +1\}$. The transmitted waveform for the mth bit of user i is given by

$$v_i^m(t) = \sum_{k=0}^{\beta-1} x_{(d_{i,m})i,k+(m-1)\beta} r[t - (kT_c + (m-1)T_b)]. \tag{4-36}$$

The transmitted waveform for user i is therefore

$$s_i(t) = \sum_{m=1}^{\infty} v_i^m(t). \tag{4-37}$$

Figure 4-8 shows the transmitter of a multi-user coherent CSK system. The overall transmitted signal of the whole system is derived by summing the signals of all individual users, i.e.,

$$s(t) = \sum_{i=1}^{N} s_i(t) = \sum_{i=1}^{N} \sum_{m=1}^{\infty} v_i^m(t). \tag{4-38}$$

4.2.1 Numerical Bit Error Probability

Corrupted by AWGN, the received signal arrives at the receiver. The demodulator for user j is depicted in Figure 4-9. The input to the demodulator is given by

$$\begin{aligned} p'(t) &= s(t) + n'(t) \\ &= \sum_{i=1}^{N}\sum_{m=1}^{\infty} v_i^m(t) + \sum_{k=0}^{\infty}\xi_k r(t-kT_c) \\ &= \sum_{i=1}^{N}\sum_{m=1}^{\infty}\sum_{k=0}^{\beta-1} x_{(d_{i,m})i,k+(m-1)\beta} r[t-(kT_c+(m-1)T_b)] + \sum_{k=0}^{\infty}\xi_k r(t-kT_c). \end{aligned} \tag{4-39}$$

For the mth received symbol, the output of the correlator$_{-j}$ at the end of the symbol period is given by

$$\begin{aligned} \mathrm{Corr}_{-j}(mT_b) &= \int_{(m-1)T_b}^{mT_b} p'(t)c_{-j}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} [\sum_{i=1}^{N} v_i^m(t) + \sum_{k=(m-1)\beta}^{m\beta-1}\xi_k r(t-kT_c)]c_{-j}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} \left[\sum_{i=1}^{N}\sum_{k=0}^{\beta-1} x_{(d_{i,m})i,k+(m-1)\beta} r[t-(kT_c+(m-1)T_b)] + \sum_{k=(m-1)\beta}^{m\beta-1}\xi_k r(t-kT_c)\right] c_{-j}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} \left[\sum_{i=1}^{N}\sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} r(t-kT_c) + \sum_{k=(m-1)\beta}^{m\beta-1}\xi_k r(t-kT_c)\right]\left[\sum_{k=(m-1)\beta}^{m\beta-1} x_{-j,k} r(t-kT_c)\right] dt. \end{aligned} \tag{4-40}$$

Therefore,

$$\mathrm{Corr}_{-j}(mT_b) = T_c\left[\sum_{i=1}^{N}\sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{-j,k} + \sum_{k=(m-1)\beta}^{m\beta-1}\xi_k x_{-j,k}\right]. \tag{4-41}$$

Similarly,

$$\mathrm{Corr}_{+j}(mT_b) = T_c\left[\sum_{i=1}^{N}\sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{+j,k} + \sum_{k=(m-1)\beta}^{m\beta-1}\xi_k x_{+j,k}\right]. \tag{4-42}$$

The input to the threshold detector at this instant is

$$z_j(mT_b) = \mathrm{Corr}_{+j}(mT_b) - \mathrm{Corr}_{-j}(mT_b)$$
$$= T_c \left[\begin{array}{l} \sum_{i=1}^{N} \sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{+j,k} + \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k x_{+j,k} \\ -\sum_{i=1}^{N} \sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{-j,k} - \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k x_{-j,k} \end{array} \right]. \tag{4-43}$$

Suppose for user j, a "+1" has been transmitted for the mth symbol, i.e., $d_{j,m} = +1$, the input of the detector will be given by

$$z_{j,+1}(mT_b) = T_c \left[\begin{array}{l} \sum_{k=(m-1)\beta}^{m\beta-1} x_{+j,k}^2 + \sum_{\substack{i=1 \\ i\neq j}}^{N} \sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{+j,k} + \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k x_{+j,k} \\ -\sum_{i=1}^{N} \sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{-j,k} - \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k x_{-j,k} \end{array} \right]. \tag{4-44}$$

Similarly, if a "–1" is transmitted, i.e., $d_{j,m} = -1$,

$$z_{j,-1}(mT_b) = T_c \left[\begin{array}{l} -\sum_{k=(m-1)\beta}^{m\beta-1} x_{-j,k}^2 + \sum_{i=1}^{N} \sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{+j,k} + \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k x_{+j,k} \\ -\sum_{\substack{i=1 \\ i\neq j}}^{N} \sum_{k=(m-1)\beta}^{m\beta-1} x_{(d_{i,m})i,k} x_{-j,k} - \sum_{k=(m-1)\beta}^{m\beta-1} \xi_k x_{-j,k} \end{array} \right]. \tag{4-45}$$

Using similar notations as in Section 4.1, equation (4-44) is expressed as

$$z_{j,+1}(mT_b) = \beta T_c [\gamma_{x_{+j}}((m-1)\beta,(m-1)\beta,\beta) + \sum_{\substack{i=1 \\ i\neq j}}^{N} \gamma_{x_{(d_{i,m})i} x_{+j}}((m-1)\beta,(m-1)\beta,\beta)$$
$$+ \gamma_{x_{+j}\xi}((m-1)\beta,(m-1)\beta,\beta) - \sum_{i=1}^{N} \gamma_{x_{(d_{i,m})i} x_{-j}}((m-1)\beta,(m-1)\beta,\beta)$$
$$- \gamma_{x_{-j}\xi}((m-1)\beta,(m-1)\beta,\beta)].$$

(4-46)

As shown in Section 2.3.4, all the terms $\gamma_{x_{+j}}, \gamma_{x_{\pm i}x_{+j}} (i = 1,2,..,N; i \neq j), \gamma_{x_{+j}\xi}$, $\gamma_{x_{\pm i}x_{-j}} (i = 1,2,..,N)$ and $\gamma_{x_{-j}\xi}$ can be modelled as normal random variables. Assume that the random variables are independent of each other. $z_{j,+1}(mT_b)$ will also be normally distributed with mean

$$\begin{aligned}
\overline{z_{j,+1}(mT_b)} &= \beta T_c[\overline{\gamma_{x_{+j}}((m-1)\beta,(m-1)\beta,\beta)} + \overline{\sum_{\substack{i=1\\ i\neq j}}^{N} \gamma_{x_{(d_{i,m})i}x_{+j}}((m-1)\beta,(m-1)\beta,\beta)} \\
&\quad + \overline{\gamma_{x_{+j}\xi}((m-1)\beta,(m-1)\beta,\beta)} - \overline{\sum_{i=1}^{N} \gamma_{x_{(d_{i,m})i}x_{-j}}((m-1)\beta,(m-1)\beta,\beta)} \\
&\quad - \overline{\gamma_{x_{-j}\xi}((m-1)\beta,(m-1)\beta,\beta)}] \\
&= \beta T_c[\overline{\gamma_{x_{+j}}((m-1)\beta,(m-1)\beta,\beta)} + \sum_{\substack{i=1\\ i\neq j}}^{N} \overline{\gamma_{x_{(d_{i,m})i}x_{+j}}((m-1)\beta,(m-1)\beta,\beta)} \\
&\quad + \overline{\gamma_{x_{+j}\xi}((m-1)\beta,(m-1)\beta,\beta)} - \sum_{i=1}^{N} \overline{\gamma_{x_{(d_{i,m})i}x_{-j}}((m-1)\beta,(m-1)\beta,\beta)} \\
&\quad - \overline{\gamma_{x_{-j}\xi}((m-1)\beta,(m-1)\beta,\beta)}]
\end{aligned}$$

(4-47)

and variance

$$
\begin{aligned}
\mathrm{var}[z_{j,+1}(mT_b)] = (\beta T_c)^2 \{ & \mathrm{var}[\gamma_{x_{+j}}((m-1)\beta,(m-1)\beta,\beta)] \\
& + \mathrm{var}\left[\sum_{\substack{i=1\\ i\neq j}}^{N} \gamma_{x(d_{i,m})i x_{+j}}((m-1)\beta,(m-1)\beta,\beta)\right] \\
& + \mathrm{var}[\gamma_{x_{+j}\xi}((m-1)\beta,(m-1)\beta,\beta)] \\
& + \mathrm{var}\left[\sum_{i=1}^{N} \gamma_{x(d_{i,m})i x_{-j}}((m-1)\beta,(m-1)\beta,\beta)\right] \\
& + \mathrm{var}[\gamma_{x_{-j}\xi}((m-1)\beta,(m-1)\beta,\beta)]\} \\
= (\beta T_c)^2 \{ & \mathrm{var}[\gamma_{x_{+j}}((m-1)\beta,(m-1)\beta,\beta)] \\
& + \sum_{\substack{i=1\\ i\neq j}}^{N} \mathrm{var}[\gamma_{x(d_{i,m})i x_{+j}}((m-1)\beta,(m-1)\beta,\beta)] \\
& + \mathrm{var}[\gamma_{x_{+j}\xi}((m-1)\beta,(m-1)\beta,\beta)] \\
& + \sum_{i=1}^{N} \mathrm{var}[\gamma_{x(d_{i,m})i x_{-j}}((m-1)\beta,(m-1)\beta,\beta)] \\
& + \mathrm{var}[\gamma_{x_{-j}\xi}((m-1)\beta,(m-1)\beta,\beta)]\}
\end{aligned}
\tag{4-48}
$$

Using the results in Table 4-1, the values of $\overline{z_{j,+1}(mT_b)}$ and $\mathrm{var}[z_{j,+1}(mT_b)]$ can now be found.

For $\beta = 100$,

$$
\begin{aligned}
\overline{z_{j,+1}(mT_b)} &= \beta T_c [0.5 + \sum_{\substack{i=1\\ i\neq j}}^{N}(0) + 0 - \sum_{i=1}^{N}(0) - 0] \\
&= 0.5\beta T_c
\end{aligned}
\tag{4-49}
$$

and

$$\begin{aligned}\mathrm{var}[z_{j,+1}(mT_b)] &= (\beta T_c)^2[1.24\mathrm{x}10^{-3} + \sum_{\substack{i=1\\ i\neq j}}^{N} 2.50\mathrm{x}10^{-3} + 5.0\mathrm{x}10^{-3}\sigma_{n'}^2 \\ &\quad + \sum_{i=1}^{N} 2.50\mathrm{x}10^{-3} + 5.0\mathrm{x}10^{-3}\sigma_{n'}^2] \\ &= (\beta T_c)^2[1.24\mathrm{x}10^{-3} + 2.50\mathrm{x}10^{-3}(2N-1) + 1.0\mathrm{x}10^{-2}\frac{N_0}{2T_c}]\end{aligned} \tag{4-50}$$

For $\beta = 1000$,

$$\begin{aligned}\overline{z_{j,+1}(mT_b)} &= \beta T_c[0.5 + \sum_{\substack{i=1\\ i\neq j}}^{N}(0) + 0 - \sum_{i=1}^{N}(0) - 0] \\ &= 0.5\beta T_c\end{aligned} \tag{4-51}$$

and

$$\begin{aligned}\mathrm{var}[z_{j,+1}(mT_b)] &= (\beta T_c)^2[1.24\mathrm{x}10^{-4} + \sum_{\substack{i=1\\ i\neq j}}^{N} 2.50\mathrm{x}10^{-4} + 5.0\mathrm{x}10^{-4}\sigma_{n'}^2 \\ &\quad + \sum_{i=1}^{N} 2.50\mathrm{x}10^{-4} + 5.0\mathrm{x}10^{-4}\sigma_{n'}^2] \\ &= (\beta T_c)^2[1.24\mathrm{x}10^{-4} + 2.50\mathrm{x}10^{-4}(2N-1) + 1.0\mathrm{x}10^{-3}\frac{N_0}{2T_c}]\end{aligned} \tag{4-52}$$

If $z_{j,+1}(mT_b)$ is larger than zero, a "+1" is decoded. Otherwise, a "–1" is detected. The error probability given a "+1" has been transmitted is given by

$$\text{Prob}(z_{j,+1}(mT_b) < 0 \mid \text{"+1" is transmitted})$$

$$= Q\left(\frac{\overline{z_{j,+1}(mT_b)}}{\sqrt{\text{var}[z_{j,+1}(mT_b)]}}\right)$$

$$= \begin{cases} Q\left(\dfrac{0.5}{\sqrt{1.24\text{x}10^{-3} + 2.50\text{x}10^{-3}(2N-1) + 1.0\text{x}10^{-2}\dfrac{N_0}{2T_c}}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{1.24\text{x}10^{-4} + 2.50\text{x}10^{-4}(2N-1) + 1.0\text{x}10^{-3}\dfrac{N_0}{2T_c}}}\right) & \beta = 1000. \end{cases} \tag{4-53}$$

Using the same procedures, it can be shown that if a "–1" is transmitted,

$$\overline{z_{j,-1}(mT_b)} = -0.5\beta T_c \quad \text{for } \beta = 100 \text{ or } 1000, \tag{4-54}$$

$$\text{var}[z_{j,-1}(mT_b)] = \begin{cases} (\beta T_c)^2\left[1.24\text{x}10^{-3} + 2.50\text{x}10^{-3}(2N-1) + 1.0\text{x}10^{-2}\dfrac{N_0}{2T_c}\right] & \beta = 100 \\ (\beta T_c)^2\left[1.24\text{x}10^{-4} + 2.50\text{x}10^{-4}(2N-1) + 1.0\text{x}10^{-3}\dfrac{N_0}{2T_c}\right] & \beta = 1000 \end{cases} \tag{4-55}$$

and

$$\text{Prob}(z_{j,-1}(mT_b) > 0 \mid \text{"−1" is transmitted})$$

$$= \begin{cases} Q\left(\dfrac{0.5}{\sqrt{1.24\text{x}10^{-3} + 2.50\text{x}10^{-3}(2N-1) + 1.0\text{x}10^{-2}\dfrac{N_0}{2T_c}}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{1.24\text{x}10^{-4} + 2.50\text{x}10^{-4}(2N-1) + 1.0\text{x}10^{-3}\dfrac{N_0}{2T_c}}}\right) & \beta = 1000. \end{cases} \tag{4-56}$$

By making use of equations (4-53) and (4-56), it can be shown easily that the overall bit error probability of a multi-user coherent CSK system under AWGN is

$$\mathrm{BEP}_{\text{multi-user}} = \begin{cases} Q\left(\dfrac{0.5}{\sqrt{1.24\text{x}10^{-3} + 2.50\text{x}10^{-3}(2N-1) + 1.0\text{x}10^{-2}\dfrac{N_0}{2T_c}}}\right) & \beta = 100 \\ Q\left(\dfrac{0.5}{\sqrt{1.24\text{x}10^{-4} + 2.50\text{x}10^{-4}(2N-1) + 1.0\text{x}10^{-3}\dfrac{N_0}{2T_c}}}\right) & \beta = 1000. \end{cases} \tag{4-57}$$

The average bit energy, as derived in Section 4.1, is equal to

$$\overline{E_b} = 0.5T_b\,. \tag{4-58}$$

Equation (4-57) is now re-written as

$$\mathrm{BEP}_{\text{multi-user}} = \begin{cases} Q\left(\dfrac{\overline{E_b}}{\sqrt{1.24\text{x}10^{-3}T_b^2 + 2.50\text{x}10^{-3}(2N-1)T_b^2 + 0.5N_0T_b}}\right) & \beta = 100 \\ Q\left(\dfrac{\overline{E_b}}{\sqrt{1.24\text{x}10^{-4}T_b^2 + 2.50\text{x}10^{-4}(2N-1)T_b^2 + 0.5N_0T_b}}\right) & \beta = 1000. \end{cases} \tag{4-59}$$

Using T_b=10^{-4}s, the BEPs are computed using equation (4-59) for a range of users and $\overline{E_b}/N_0$ values. The results are tabulated in Table 4-4. With an increasing number of users transmitting their chaotic signals at the same time, more interference will be introduced into the system which will cause more errors. Therefore, as shown in the table, the BEP increases with an increasing number of users. Moreover, as in the single-user case, the BEP decreases with increasing $\overline{E_b}/N_0$ and for the same $\overline{E_b}/N_0$, the BEP for β= 100 is worse than that for β= 1000. Note that in a multi-user system, when

the number of users increases, it is possible that the performance of the system will be limited by the interference caused by the users and not by the noise power. For example, for a spreading factor of 100 and with 20 users in the system, the BEP will improve gradually from 0.20 as $\overline{E_b}/N_0$ increases from 0dB. No matter how much we increase the signal power of the users, however, the BEP cannot be better than 0.056. On the other hand, by using a large spreading factor, in this case 1000, such limitation can be removed.

4.2.2 Simulations

Computer simulations have been performed based on the transmitter model in Figures 4-7 and 4-8, and the demodulator in Figure 4-9. The bit period is assumed to be 10^{-4} s with β = 100 and 1000. For each of the different $\overline{E_b}/N_0$ values simulated, 10,000 bits have been transmitted for each user and the average BEPs are tabulated in Table 4-5.

4.2.3 Comparisons

The numerical and simulated BEPs are plotted against $\overline{E_b} / N_0$ in Figures 4-10 and 4-11 for β = 100 and 1000 respectively. In both cases, the numerical BEPs agree well with the simulated results. Hence, we can conclude the numerical derivation provides an accurate means to estimate the BEPs for a multi-user CSK communications system.

4.3 Comparison with Conventional Spread Spectrum Communications System

A conventional spread spectrum communications system using Gold code [Pete 95] as the spreading code has been simulated. Gold codes are well-known for its well-defined discrete cross-correlation values given by

$$\sum_{m=1}^{M} G_u(m)G_v(m) = \begin{cases} 0.1181,\ -0.0079 \text{ or } -0.1339 & M = 127 \\ 0.0616, -0.0010 \text{ or } -0.0635 & M = 1023 \end{cases} \tag{4-60}$$

where G_u and G_v are Gold sequences belonging to the same set of Gold codes with a period of M. The channel is assumed to be an AWGN channel with psd $N_0/2$. In the first set of simulations, the chip duration T_c is fixed at 10^{-6}s and the spreading factor used is 127. The number of users ranges from 1 to 50 and 10,000 bits are sent by each user. The average BEPs are shown in Table 4-6(a) for various $\overline{E_b}/N_0$. For the second set of simulations, T_c is fixed at 10^{-7}s and the spreading factor used is 1023. The results are shown in Table 4-6(b).

The BEPs of the multi-user CSK and the conventional spread spectrum communications systems are plotted in Figures 4-12 and 4-13. It can be observed that under an AWGN channel, the performance of the conventional spread spectrum system is significantly better than the CSK system.

On the other hand, conventional spread spectrum communications systems can be decoded relatively easily even by an unintended opponent. On the contrary, in CSK, if the chaotic signals are not known, it would be extremely difficult to decode the binary data. Therefore, CSK can provide a more secured means of communications.

4.4 Conclusions

In this chapter, we have reviewed the operations of a single-user coherent CSK communications system. Using a cubic map as an illustration to generate chaos, we derive the numerical bit error probabilities for various average bit energy to noise power spectral density ratio ($\overline{E_b} / N_0$). Simulations are performed and the simulated BEPs show good consistence with the numerical BEPs.

We then extend our analysis on coherent CSK system to a multi-user environment. Numerical BEPs are again derived and compared with the simulation results. It is found that the numerical derivation on the BEPs provides a very good estimation of the actual performance. In general, the BEP decreases with increasing $\overline{E_b} / N_0$ which is expected. Moreover, the BEPs can be reduced for the same $\overline{E_b} / N_0$ by using a higher spreading ratio. In a multi-user environment, more interference will be introduced into the system when more users are transmitting at the same time. Hence, the interference between users can sometimes pose a lower limit on the BEP.

Finally, the performance of the coherent CSK system is compared with a conventional spread spectrum system. Results show that the conventional spread spectrum system can achieve a lower BEP. Nevertheless, CSK can provide a more secured communications link because without prior knowledge of the chaotic signals, it is extremely difficult, if not impossible, to synchronize with the noise-like incoming signal and hence decode it.

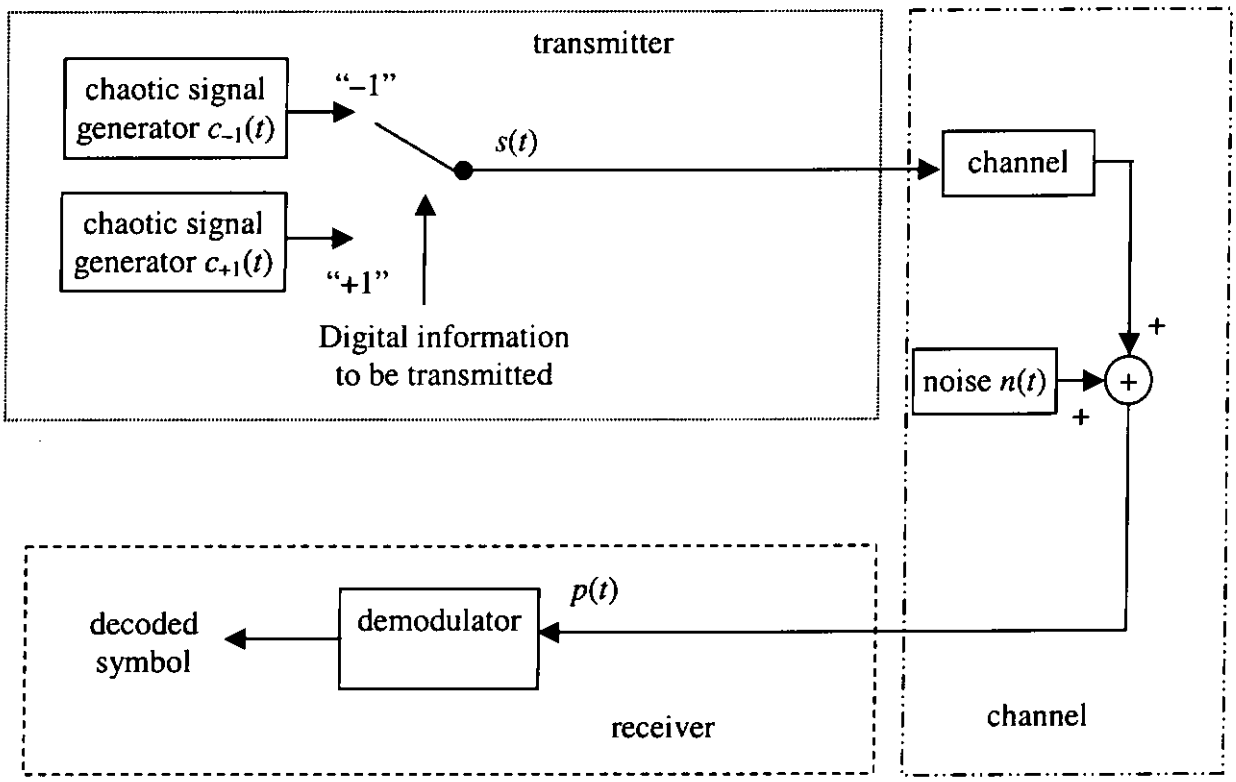


Figure 4-1 Chaos shift keying digital communications system

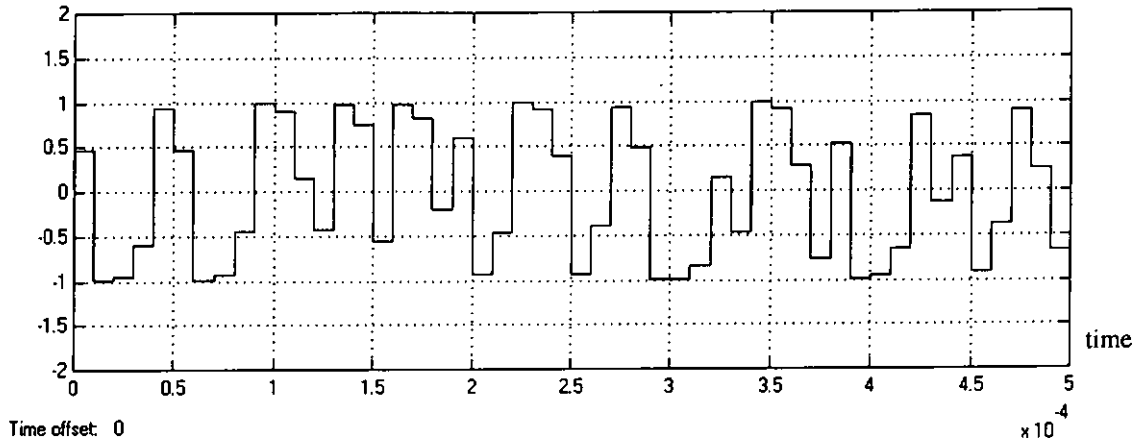


Figure 4-2(a) Output of chaotic signal generator $c_{-1}(t)$

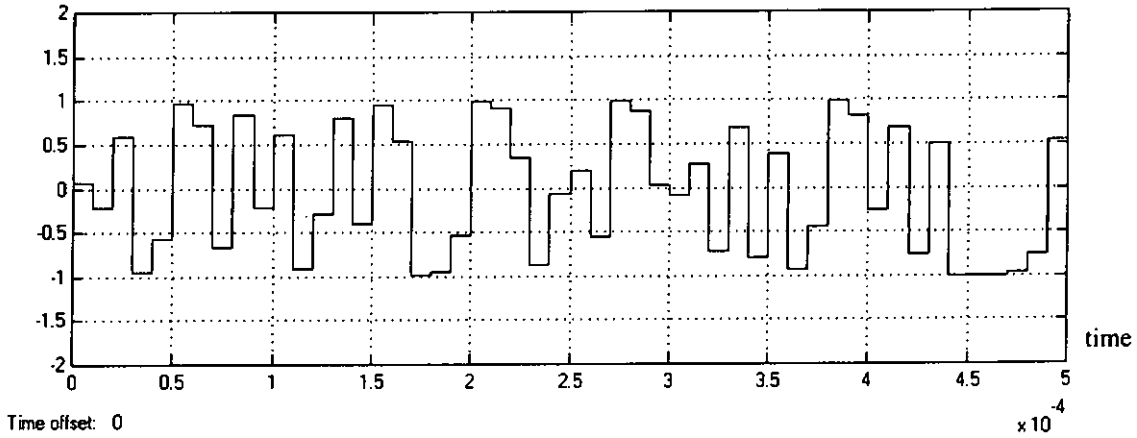


Figure 4-2(b) Output of chaotic signal generator $c_{+1}(t)$

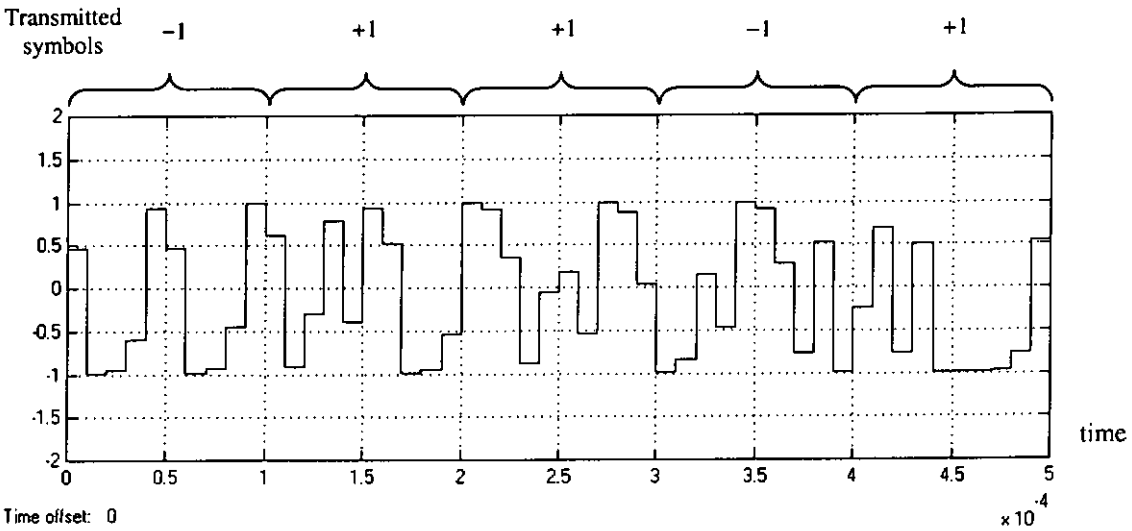


Figure 4-2(c) Transmitted waveform $s(t)$

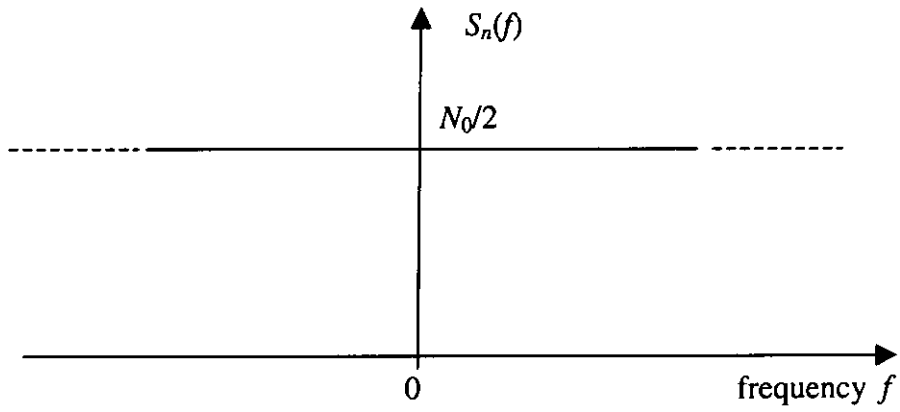


Figure 4-3 Power spectrum of additive white Gaussian noise

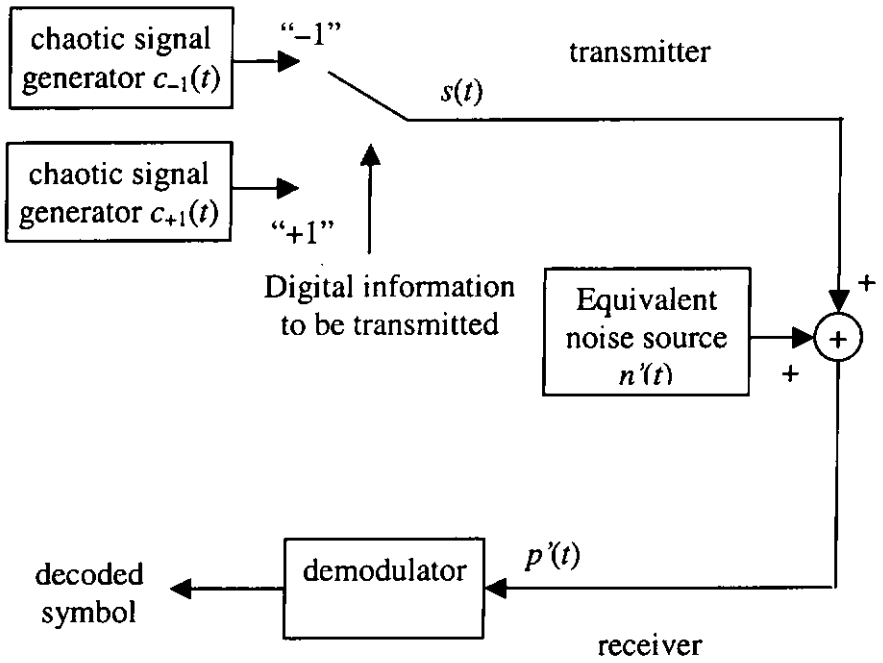


Figure 4-4 Equivalent model of a chaos shift keying digital communications system

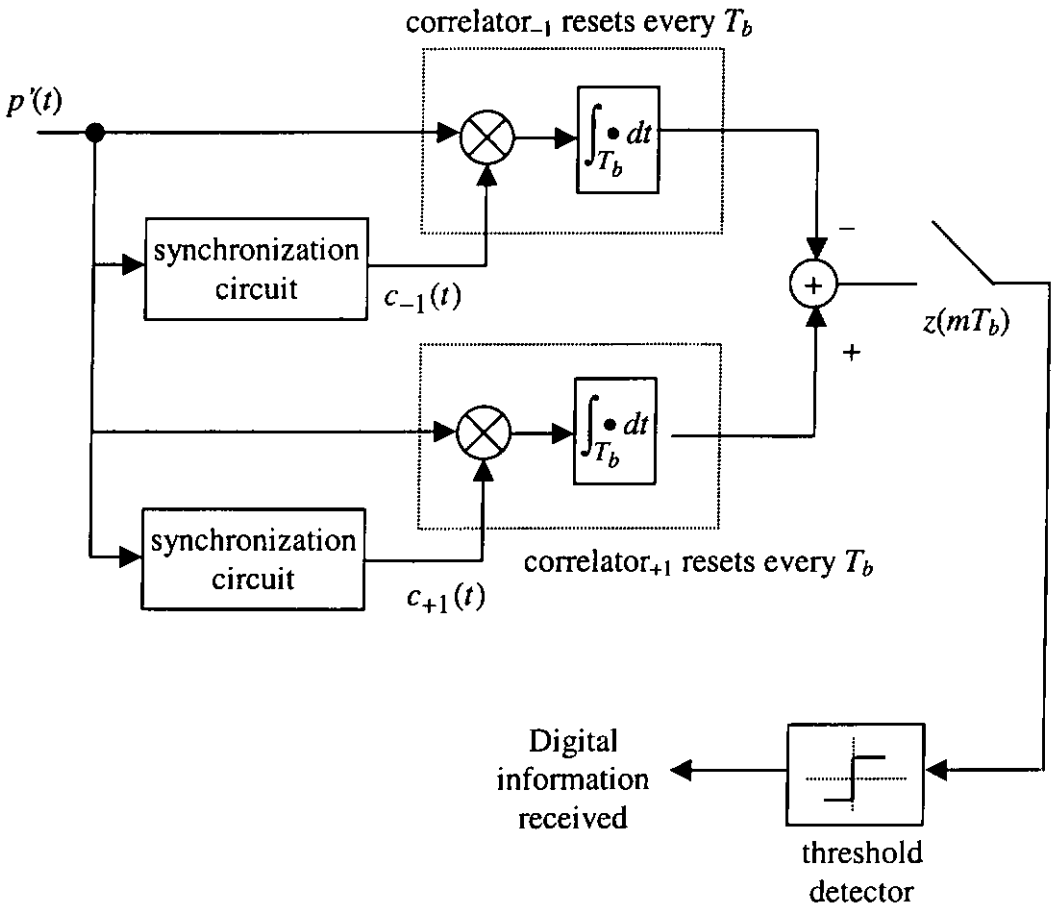


Figure 4-5 Coherent CSK demodulator

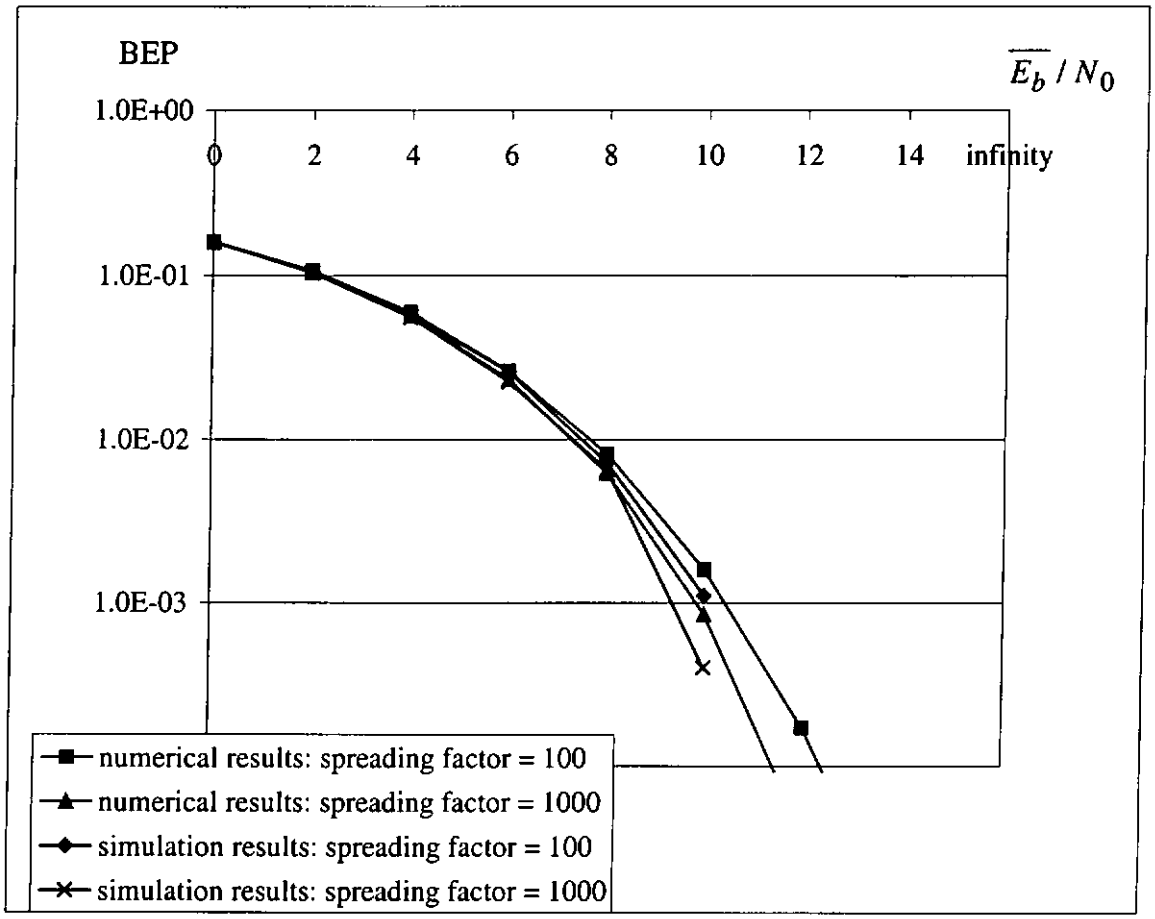


Figure 4-6 Numerical and simulated bit error probabilities against $\overline{E_b} / N_0$ in a single-user coherent CSK system

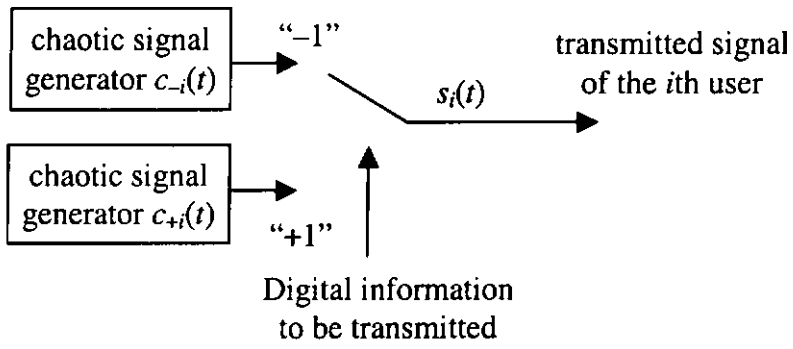


Figure 4-7 Transmitter of the ith user in a multi-user coherent CSK digital communications system

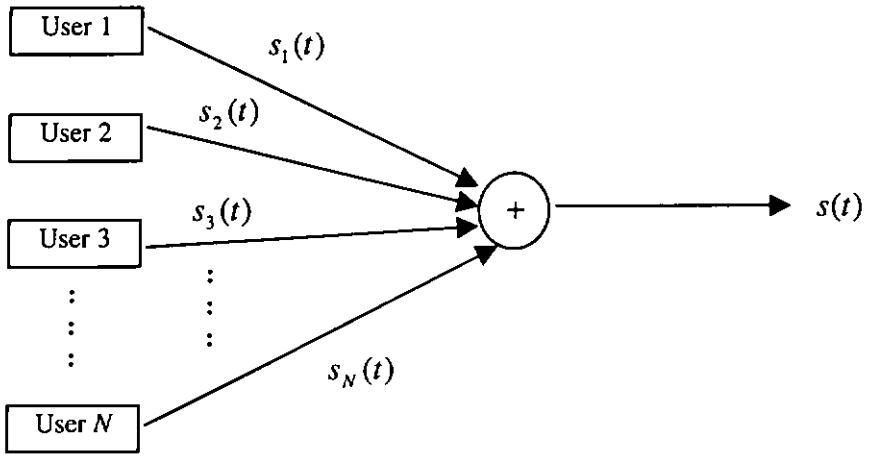


Figure 4-8 Transmitter of a multi-user coherent CSK digital communication system

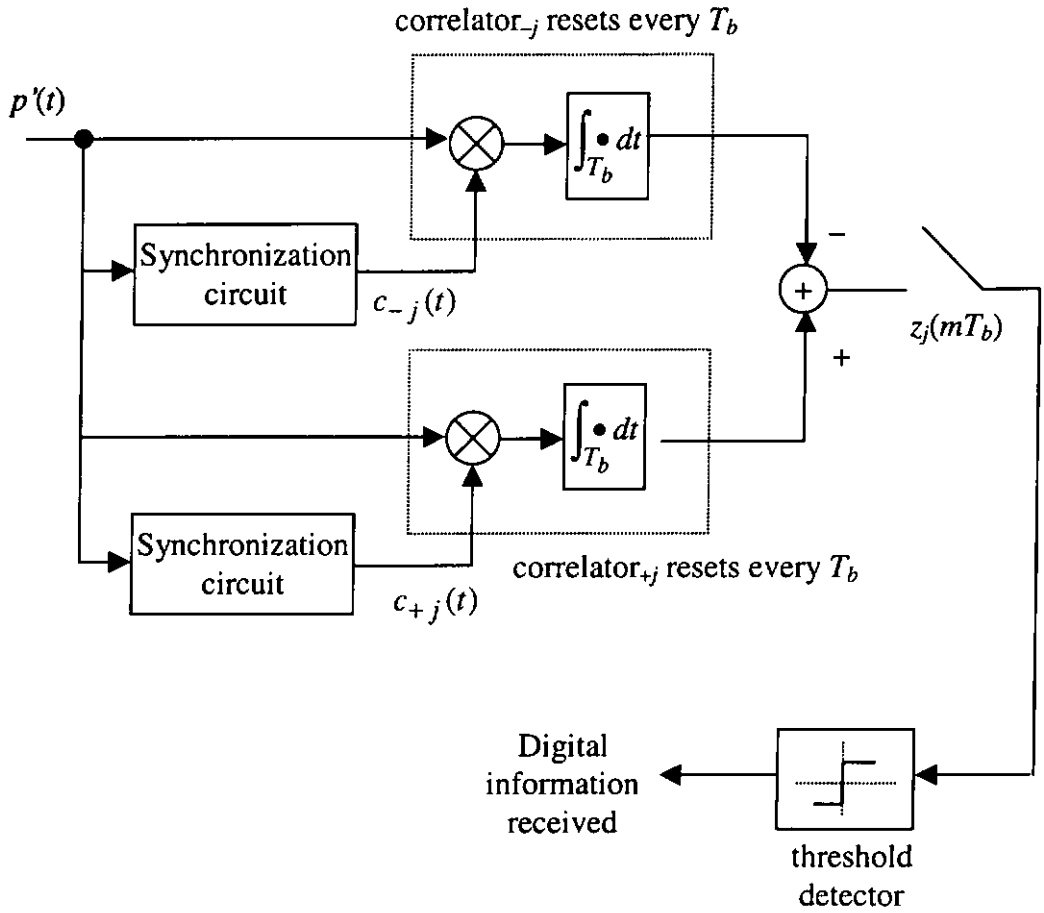


Figure 4-9 Coherent demodulator for user j in a multi-user coherent CSK communications system

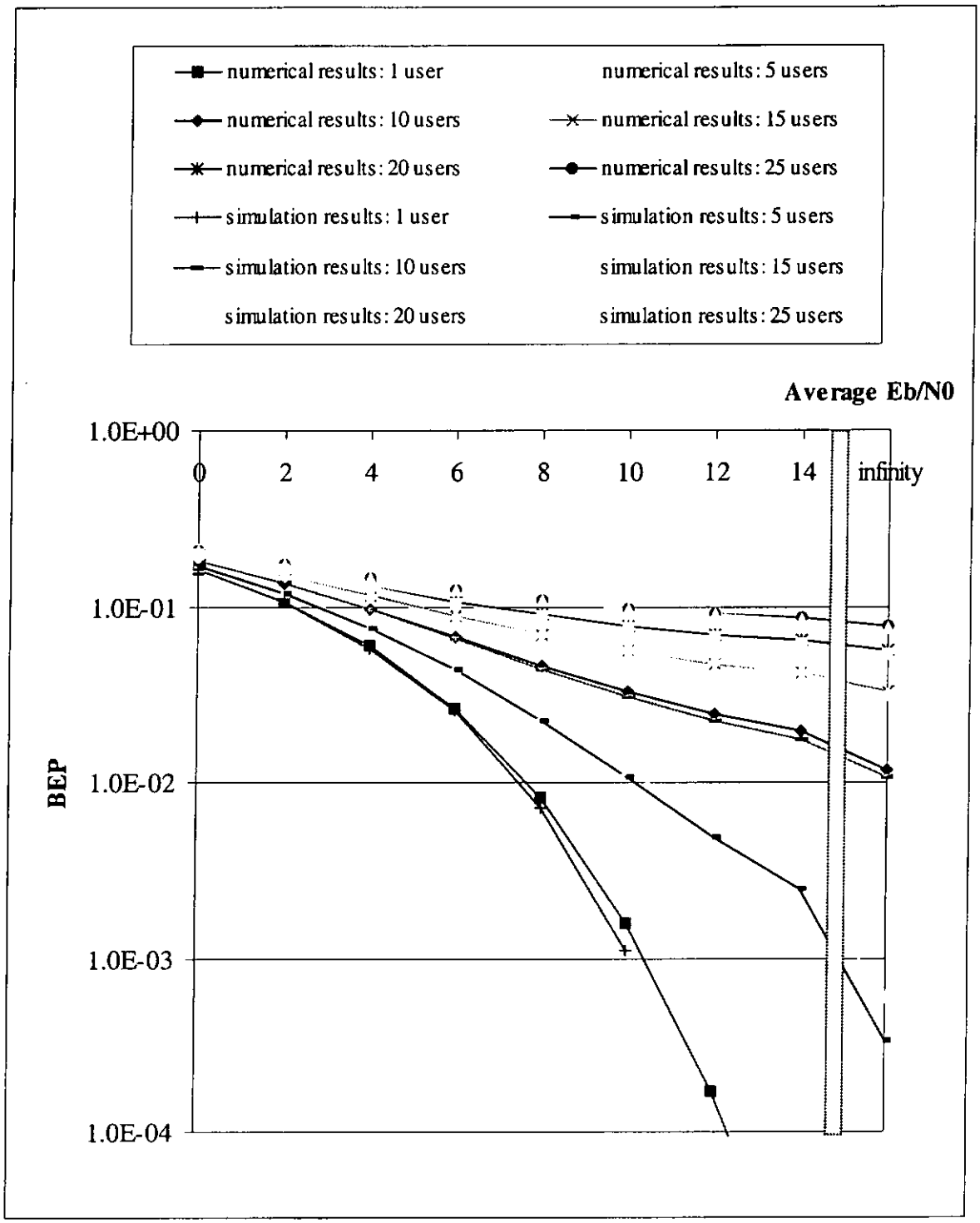


Figure 4-10(a) Numerical and simulated bit error probabilities against $\overline{E_b} / N_0$ in a multi-user coherent CSK system (1~25 users, spreading factor = 100)

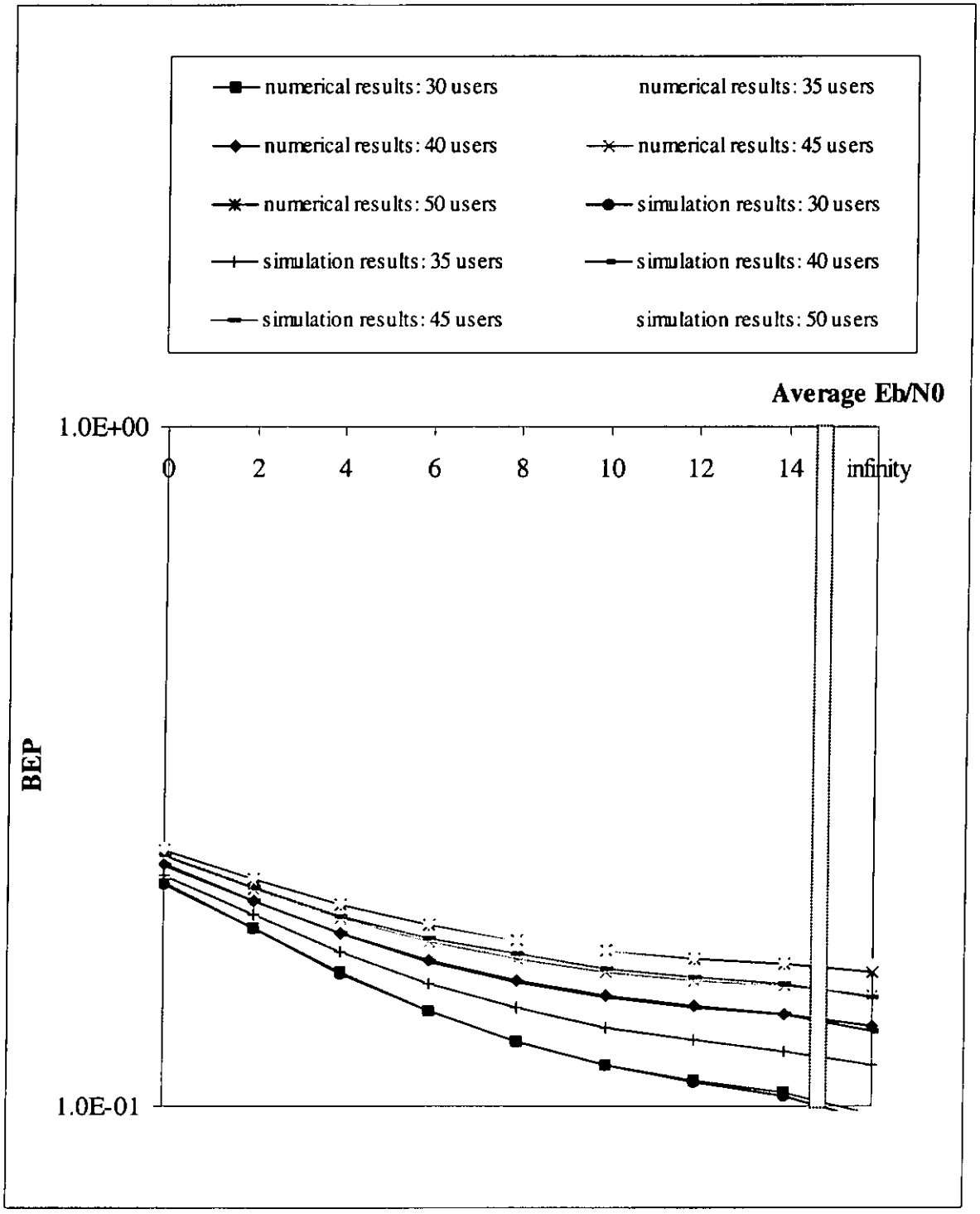


Figure 4-10(b) Numerical and simulated bit error probabilities against $\overline{E_b} / N_0$ in a multi-user coherent CSK system (30~50 users, spreading factor = 100)

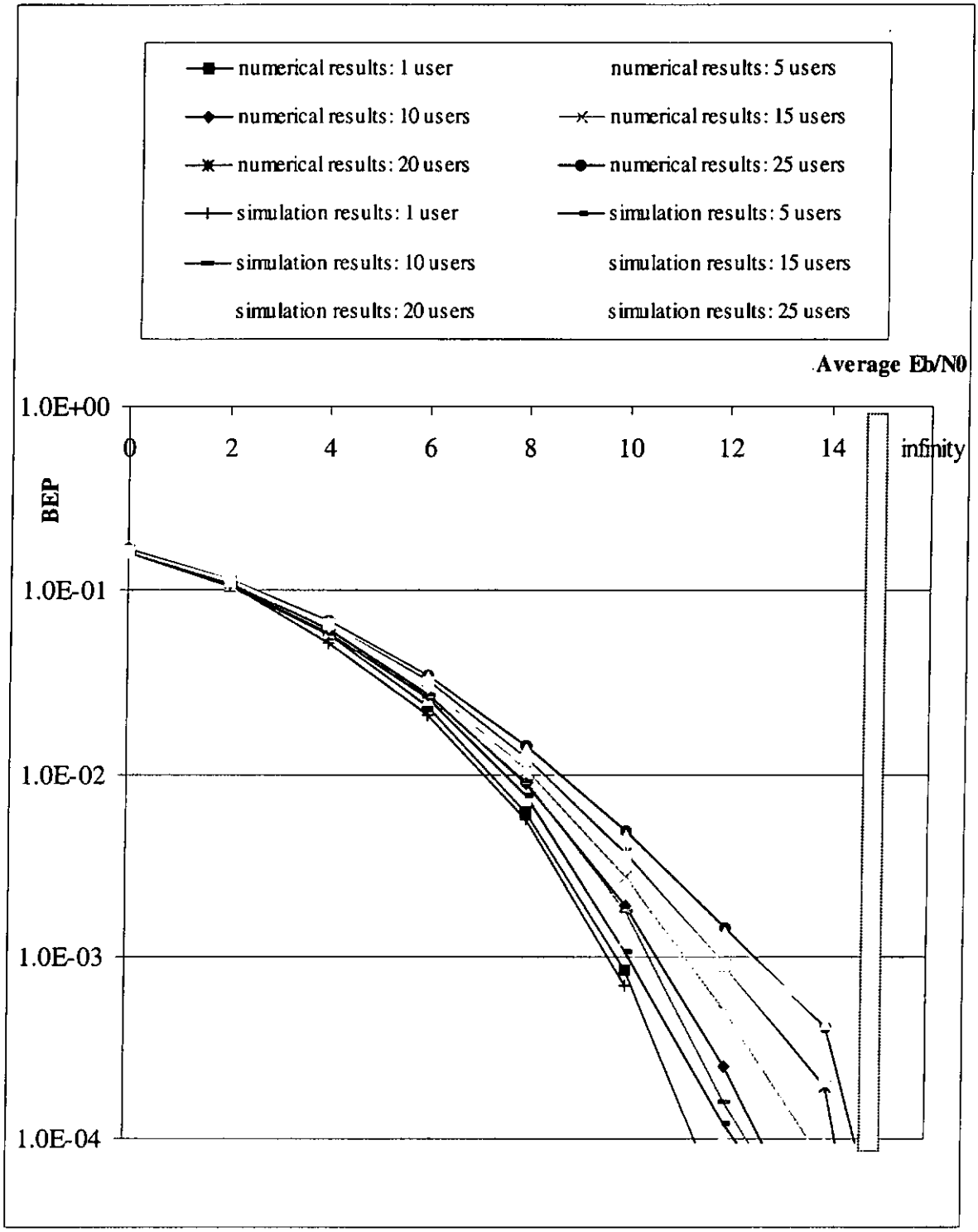


Figure 4-11(a) Numerical and simulated bit error probabilities against $\overline{E_b} / N_0$ in a multi-user coherent CSK system (1~25 users, spreading factor = 1000)

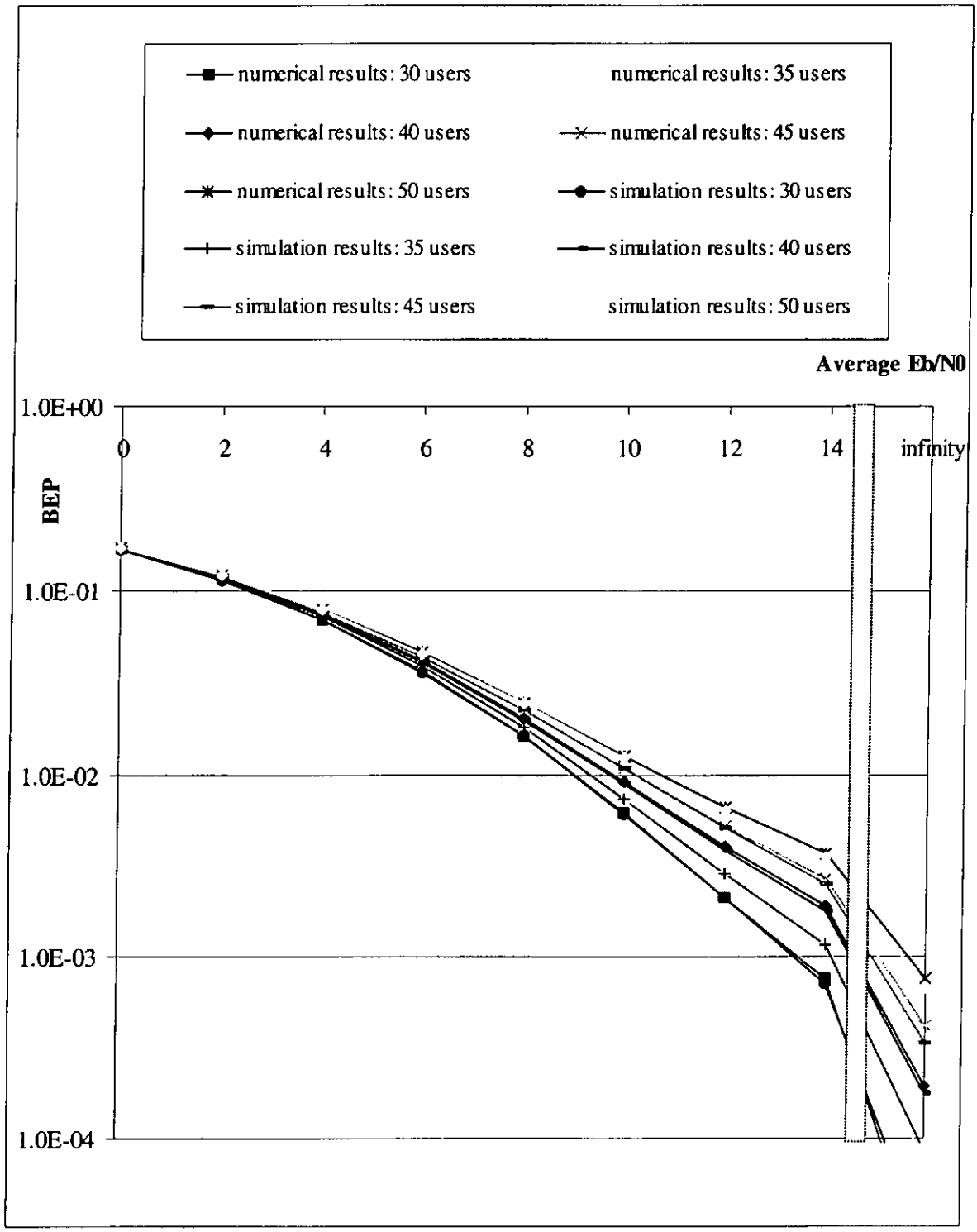


Figure 4-11(b) Numerical and simulated bit error probabilities against $\overline{E_b} / N_0$ in a multi-user coherent CSK system (30~50 users, spreading factor = 1000)

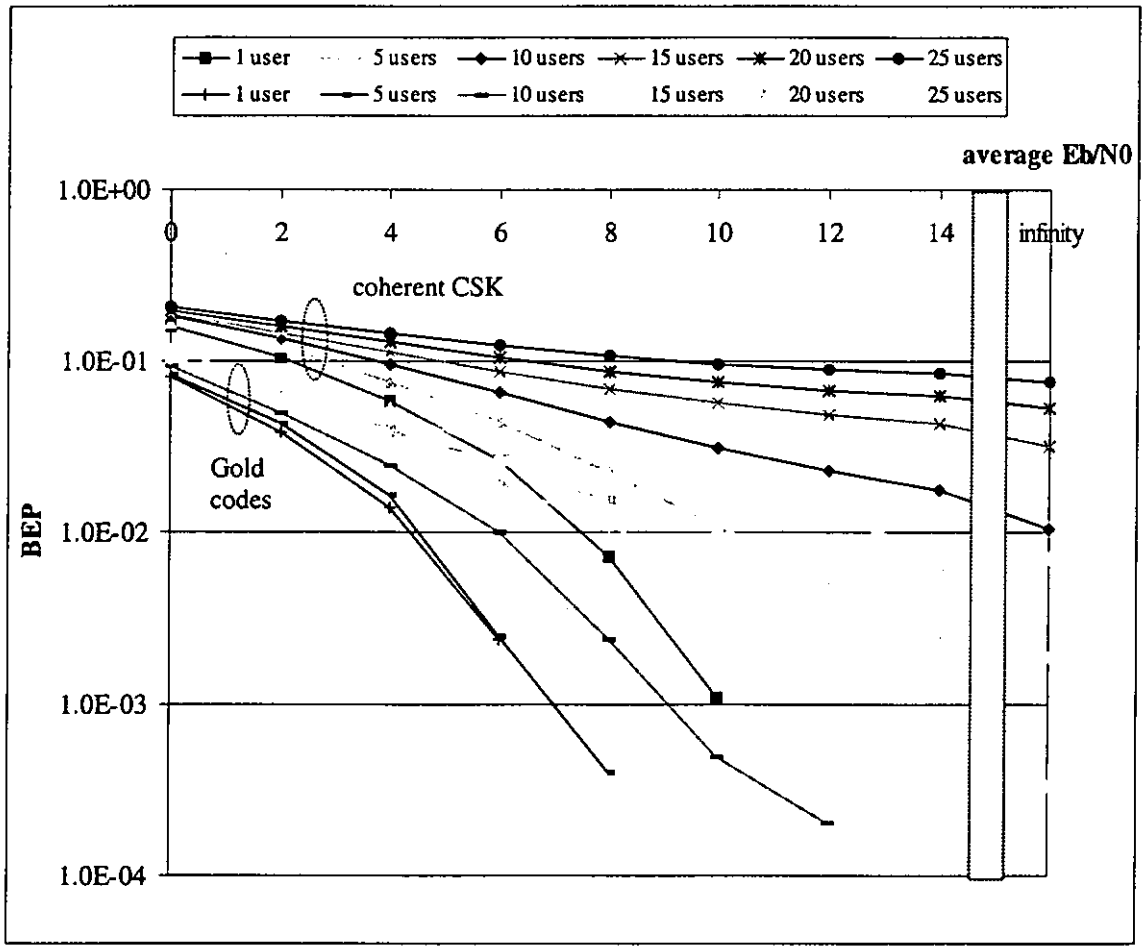


Figure 4-12(a) Simulated BEPs against $\overline{E_b} / N_0$ (1~25 users)
(spreading factor of CSK = 100, spreading factor using Gold code = 127)

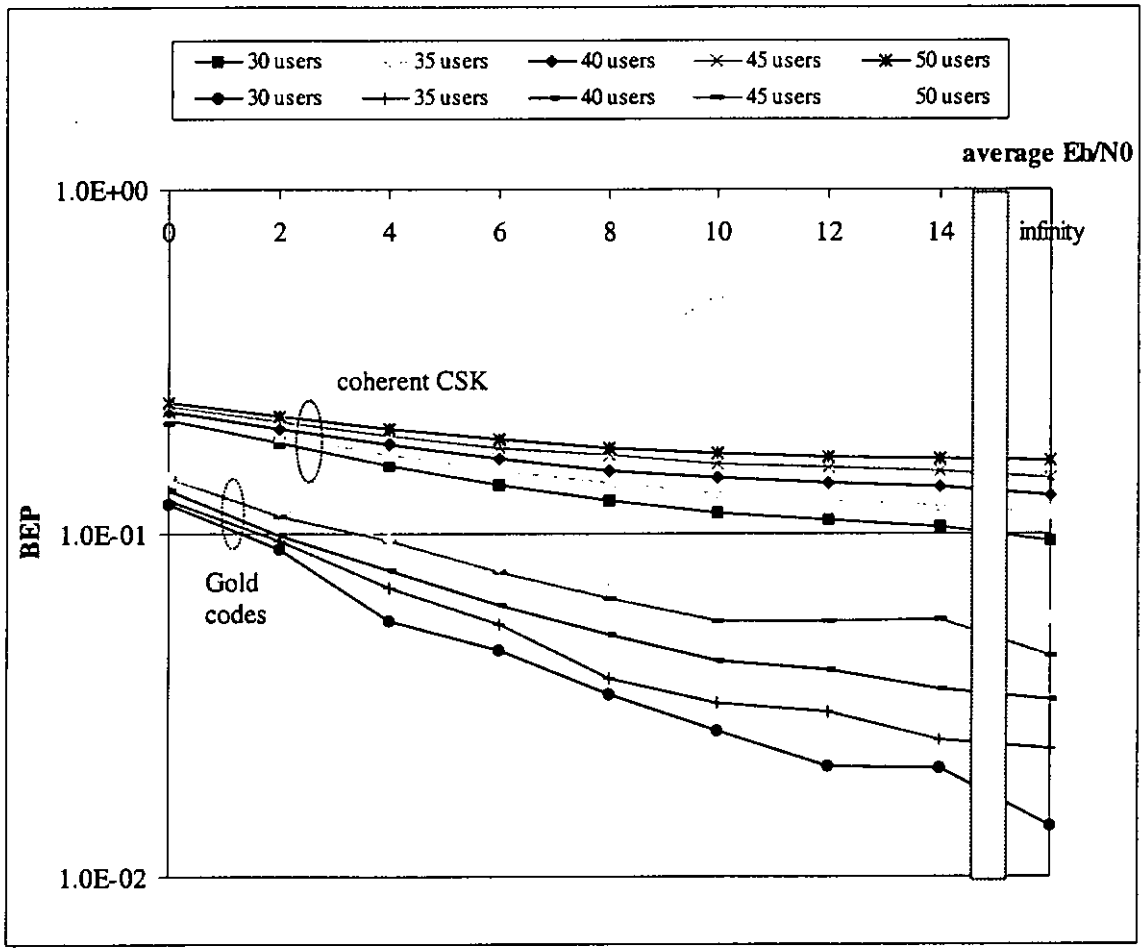


Figure 4-12(b) Simulated BEPs against $\overline{E_b} / N_0$ (30~50 users)
(spreading factor of CSK = 100, spreading factor using Gold code = 127)

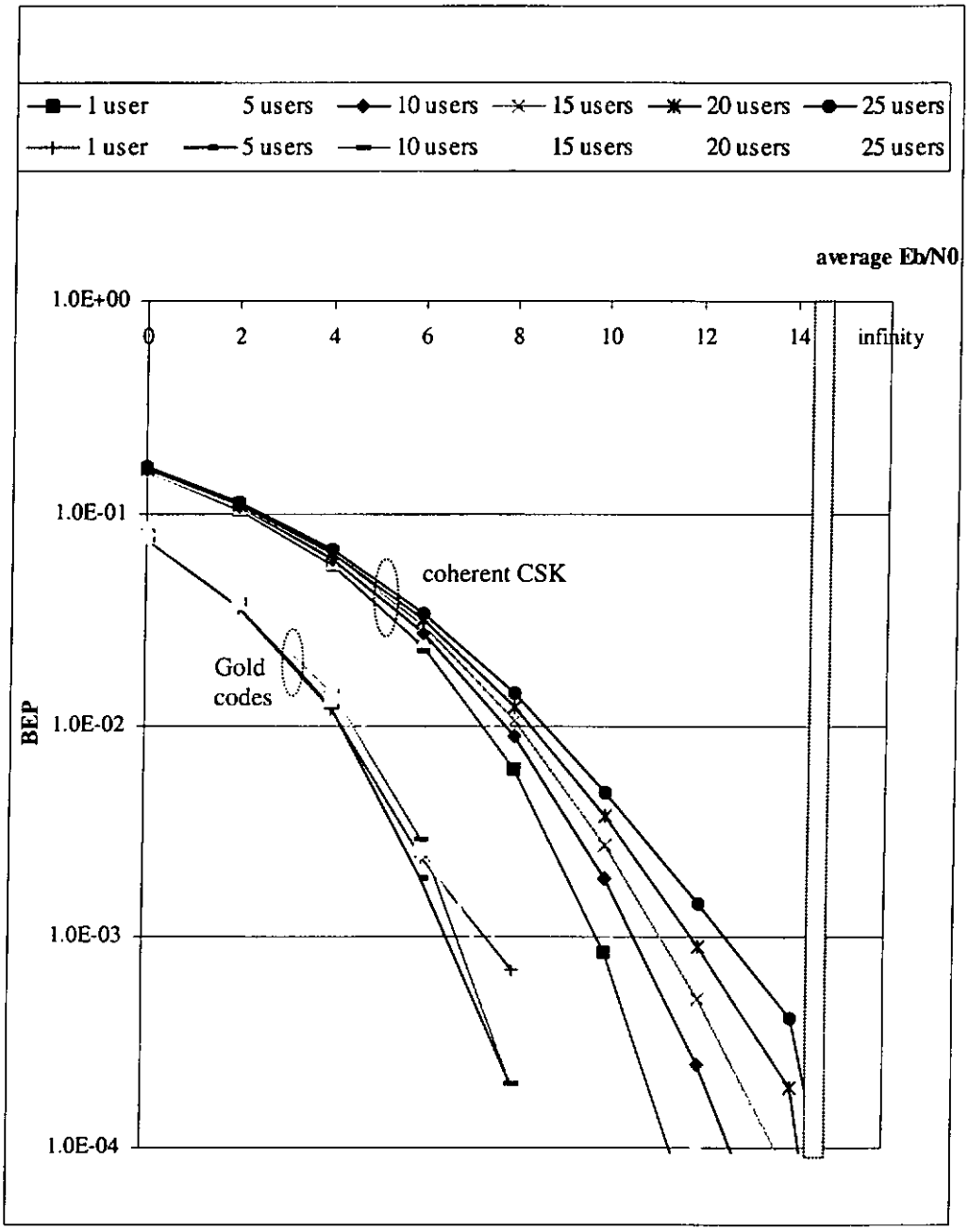


Figure 4-13(a) Simulated BEPs against $\overline{E_b} / N_0$ (1~25 users)
(spreading factor of CSK = 1000, spreading factor using Gold code = 1023)

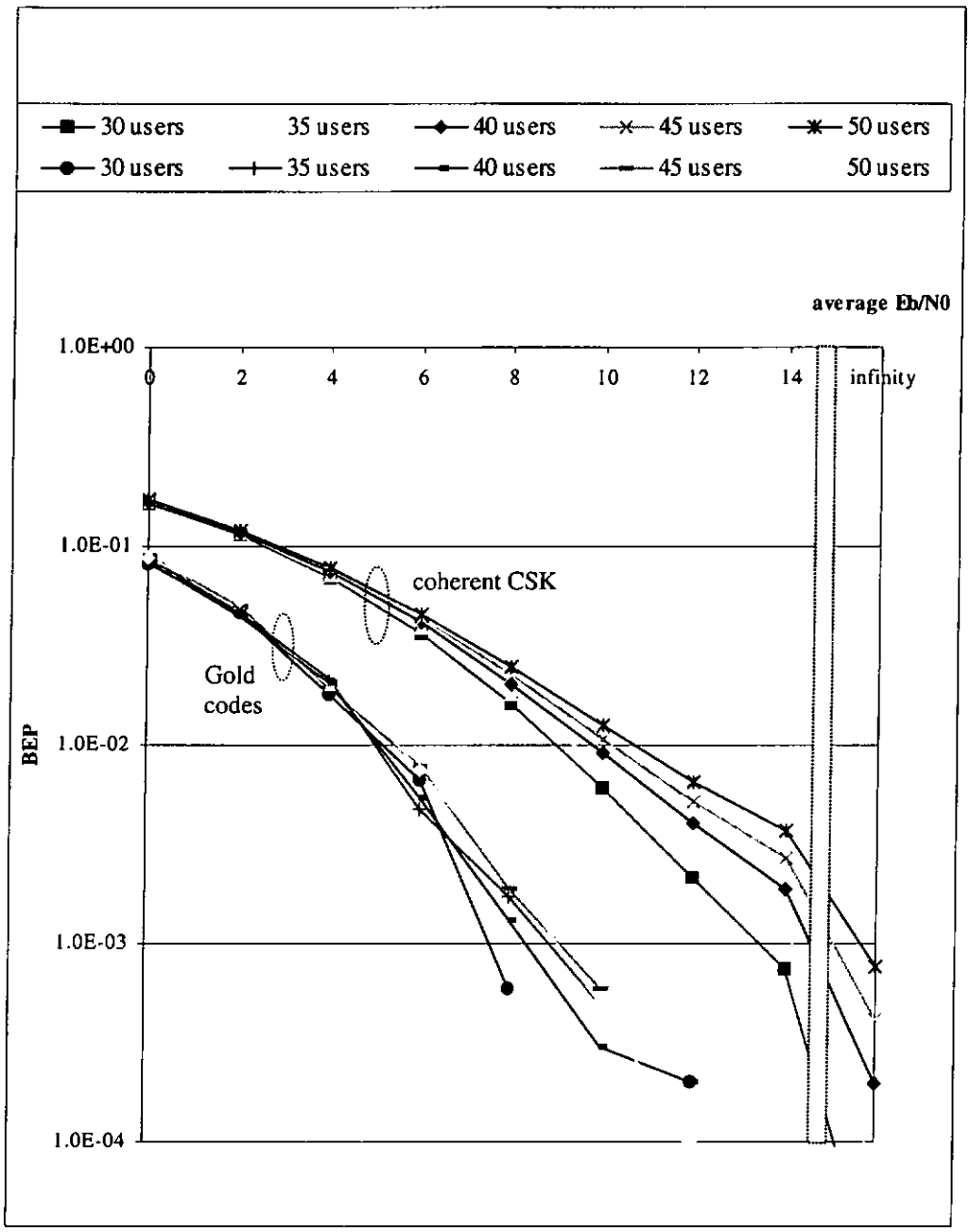


Figure 4-13(b) Simulated BEPs against $\overline{E_b} / N_0$ (30~50 users)
(spreading factor of CSK = 1000, spreading factor using Gold code = 1023)

Type of partial discrete correlation function	Correlation function	Mean	Variance
Auto-correlation with $k= l$	$\gamma_x(k,k,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}^2$	$m_{x,k=l}=\begin{cases}0.5 & L=100\\ 0.5 & L=1000\end{cases}$	$\sigma_{x,k=l}^2=\begin{cases}1.24\text{x}10^{-3} & L=100\\ 1.24\text{x}10^{-4} & L=1000\end{cases}$
Auto-correlation with $k\neq l$	$\gamma_x(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}x_{l+n}$	$m_{x,k\neq l}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{x,k\neq l}^2=\begin{cases}2.50\text{x}10^{-3} & L=100\\ 2.50\text{x}10^{-4} & L=1000\end{cases}$
Cross-correlation	$\gamma_{xx'}(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}x'_{l+n}$	$m_{xx'}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{xx'}^2=\begin{cases}2.50\text{x}10^{-3} & L=100\\ 2.50\text{x}10^{-4} & L=1000\end{cases}$
Cross-correlation with normal random sequences with zero mean and unit variance	$\gamma_{x\phi}(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}\phi_{l+n}$	$m_{x\phi}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{x\phi}^2=\begin{cases}5.0\text{x}10^{-3} & L=100\\ 5.0\text{x}10^{-4} & L=1000\end{cases}$
Cross-correlation with normal random sequences with zero mean and variance σ_λ^2	$\gamma_{x\lambda}(k,l,L)=\frac{1}{L}\sum_{n=0}^{L-1}x_{k+n}\lambda_{l+n}$	$m_{x\lambda}=\begin{cases}0 & L=100\\ 0 & L=1000\end{cases}$	$\sigma_{x\lambda}^2=\begin{cases}5.0\text{x}10^{-3}\sigma_\lambda^2 & L=100\\ 5.0\text{x}10^{-4}\sigma_\lambda^2 & L=1000\end{cases}$

Table 4-1 Means and variances of the partial discrete correlation functions of the chaotic series

$\overline{E_b} / N_0$ in dB	Spreading factor β	
	100	1000
0	0.1605	0.1588
2	0.1067	0.1043
4	0.0599	0.0568
6	0.0263	0.0233
8	0.0082	0.0062
10	0.0016	0.0008
12	0.0002	0.0000
14	0.0000	0.0000
∞	0.0000	0.0000

Table 4-2 Numerical bit error probabilities of a single-user coherent CSK system for various $\overline{E_b} / N_0$

$\overline{E_b}/N_0$ in dB	Spreading factor β	
	100	1000
0	0.1604	0.1596
2	0.1050	0.1038
4	0.0577	0.0558
6	0.0259	0.0225
8	0.0072	0.0065
10	0.0011	0.0004
12	0.0000	0.0000
14	0.0000	0.0000
∞	0.0000	0.0000

Table 4-3 Simulated bit error probabilities of a single-user coherent CSK system for various $\overline{E_b}/N_0$

$\overline{E_b}/N_0$ in dB	Number of users										
	1	5	10	15	20	25	30	35	40	45	50
0	0.1605	0.1696	0.1801	0.1898	0.1986	0.2067	0.2142	0.2212	0.2277	0.2338	0.2395
2	0.1067	0.1203	0.1356	0.1493	0.1618	0.1730	0.1832	0.1926	0.2012	0.2091	0.2164
4	0.0599	0.0772	0.0971	0.1148	0.1307	0.1450	0.1578	0.1694	0.1800	0.1896	0.1984
6	0.0263	0.0446	0.0672	0.0880	0.1067	0.1235	0.1385	0.1520	0.1641	0.1751	0.1852
8	0.0082	0.0235	0.0463	0.0688	0.0894	0.1080	0.1246	0.1395	0.1529	0.1650	0.1759
10	0.0016	0.0118	0.0328	0.0558	0.0776	0.0974	0.1152	0.1310	0.1452	0.1580	0.1696
12	0.0002	0.0059	0.0245	0.0473	0.0698	0.0903	0.1088	0.1254	0.1402	0.1535	0.1655
14	0.0000	0.0032	0.0195	0.0420	0.0647	0.0857	0.1047	0.1217	0.1369	0.1505	0.1628
∞	0.0000	0.0006	0.0118	0.0328	0.0558	0.0776	0.0974	0.1152	0.1310	0.1452	0.1580

Table 4-4(a) Numerical BEPs of a multi-user coherent CSK system for various $\overline{E_b}/N_0$ with a spreading factor of 100

$\overline{E_b}/N_0$ in dB	Number of users										
	1	5	10	15	20	25	30	35	40	45	50
0	0.1588	0.1598	0.1610	0.1622	0.1633	0.1645	0.1656	0.1668	0.1679	0.1690	0.1701
2	0.1043	0.1057	0.1075	0.1093	0.1110	0.1127	0.1144	0.1161	0.1177	0.1194	0.1210
4	0.0568	0.0586	0.0609	0.0631	0.0653	0.0675	0.0697	0.0718	0.0739	0.0761	0.0782
6	0.0233	0.0251	0.0273	0.0295	0.0318	0.0341	0.0364	0.0387	0.0410	0.0433	0.0456
8	0.0062	0.0073	0.0089	0.0105	0.0123	0.0142	0.0161	0.0181	0.0202	0.0223	0.0245
10	0.0008	0.0013	0.0019	0.0027	0.0037	0.0049	0.0061	0.0076	0.0091	0.0108	0.0126
12	0.0000	0.0001	0.0003	0.0005	0.0009	0.0014	0.0021	0.0030	0.0040	0.0052	0.0066
14	0.0000	0.0000	0.0000	0.0001	0.0002	0.0004	0.0008	0.0012	0.0019	0.0027	0.0037
∞	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001	0.0002	0.0004	0.0008

Table 4-4(b) Numerical BEPs of a multi-user coherent CSK system for various $\overline{E_b}/N_0$ with a spreading factor of 1000

$\overline{E_b}/N_0$ in dB	Number of users										
	1	5	10	15	20	25	30	35	40	45	50
0	0.1604	0.1692	0.1824	0.1883	0.1970	0.2065	0.2128	0.2198	0.2267	0.2343	0.2405
2	0.1050	0.1196	0.1363	0.1471	0.1603	0.1722	0.1828	0.1916	0.2010	0.2102	0.2178
4	0.0577	0.0760	0.0961	0.1137	0.1294	0.1441	0.1568	0.1693	0.1798	0.1911	0.2004
6	0.0259	0.0441	0.0655	0.0872	0.1043	0.1225	0.1383	0.1517	0.1636	0.1776	0.1861
8	0.0072	0.0222	0.0436	0.0689	0.0879	0.1070	0.1248	0.1400	0.1523	0.1678	0.1765
10	0.0011	0.0106	0.0309	0.0563	0.0755	0.0961	0.1148	0.1302	0.1451	0.1594	0.1705
12	0.0000	0.0049	0.0226	0.0480	0.0671	0.0896	0.1087	0.1249	0.1401	0.1547	0.1662
14	0.0000	0.0025	0.0176	0.0426	0.0620	0.0844	0.1037	0.1205	0.1367	0.1512	0.1637
∞	0.0000	0.0003	0.0106	0.0313	0.0534	0.0759	0.0949	0.1151	0.1291	0.1444	0.1618

Table 4-5(a) Simulated BEPs of a multi-user coherent CSK system for various $\overline{E_b}/N_0$ with a spreading factor of 100

$\overline{E_b}/N_0$ in dB	Number of users										
	1	5	10	15	20	25	30	35	40	45	50
0	0.1620	0.1597	0.1596	0.1631	0.1630	0.1637	0.1660	0.1661	0.1669	0.1700	0.1702
2	0.1060	0.1051	0.1086	0.1107	0.1125	0.1118	0.1141	0.1155	0.1166	0.1201	0.1209
4	0.0510	0.0584	0.0602	0.0631	0.0649	0.0665	0.0690	0.0716	0.0732	0.0761	0.0779
6	0.0208	0.0260	0.0265	0.0291	0.0314	0.0336	0.0360	0.0388	0.0403	0.0431	0.0451
8	0.0057	0.0077	0.0090	0.0103	0.0121	0.0136	0.0160	0.0179	0.0197	0.0224	0.0241
10	0.0007	0.0011	0.0018	0.0025	0.0035	0.0046	0.0060	0.0074	0.0090	0.0109	0.0123
12	0.0000	0.0001	0.0002	0.0005	0.0009	0.0014	0.0021	0.0029	0.0039	0.0051	0.0063
14	0.0000	0.0000	0.0000	0.0001	0.0002	0.0004	0.0007	0.0012	0.0018	0.0025	0.0035
∞	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001	0.0002	0.0003	0.0007

Table 4-5(b) Simulated BEPs of a multi-user coherent CSK system for various $\overline{E_b}/N_0$ with a spreading factor of 1000

$\overline{E_b}/N_0$ in dB	Number of users										
	1	5	10	15	20	25	30	35	40	45	50
0	0.0810	0.0830	0.0926	0.1012	0.1037	0.1148	0.1214	0.1235	0.1329	0.1454	0.1439
2	0.0386	0.0427	0.0500	0.0647	0.0689	0.0739	0.0893	0.0953	0.0986	0.1119	0.1172
4	0.0139	0.0162	0.0246	0.0363	0.0395	0.0531	0.0554	0.0688	0.0776	0.0953	0.0956
6	0.0024	0.0025	0.0099	0.0194	0.0256	0.0290	0.0455	0.0543	0.0618	0.0766	0.0795
8	0.0000	0.0004	0.0024	0.0108	0.0149	0.0211	0.0337	0.0374	0.0503	0.0643	0.0709
10	0.0000	0.0000	0.0005	0.0062	0.0103	0.0156	0.0264	0.0318	0.0423	0.0552	0.0682
12	0.0000	0.0000	0.0002	0.0030	0.0080	0.0110	0.0209	0.0302	0.0397	0.0555	0.0628
14	0.0000	0.0000	0.0000	0.0022	0.0062	0.0088	0.0207	0.0250	0.0352	0.0559	0.0627
∞	0	0	0	0	0.0019	0.0071	0.0141	0.0234	0.0327	0.0436	0.0566

Table 4-6(a) Simulated BEPs of a conventional spread spectrum communication system for various $\overline{E_b}/N_0$ with a spreading factor of 127

$\overline{E_b} / N_0$ in dB	Number of users										
	1	5	10	15	20	25	30	35	40	45	50
0	0.0750	0.0763	0.0819	0.0803	0.0777	0.0836	0.0821	0.0873	0.0830	0.0892	0.0882
2	0.0363	0.0373	0.0388	0.0386	0.0377	0.0390	0.0468	0.0461	0.0446	0.0492	0.0527
4	0.0120	0.0121	0.0146	0.0149	0.0130	0.0150	0.0181	0.0216	0.0208	0.0193	0.0244
6	0.0024	0.0019	0.0029	0.0025	0.0026	0.0046	0.0066	0.0048	0.0054	0.0078	0.0074
8	0.0007	0.0002	0.0002	0.0008	0.0005	0.0003	0.0006	0.0017	0.0013	0.0019	0.0022
10	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0005	0.0003	0.0006	0.0005
12	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0002	0.0000	0.0002	0.0000	0.0001
14	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
∞	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Table 4-6(b) Simulated BEPs of a conventional spread spectrum communication system for various $\overline{E_b} / N_0$ with a spreading factor of 1023

CHAPTER 5

DIFFERENTIAL CHAOS SHIFT KEYING IN A MULTI-USER ENVIRONMENT

In the previous chapter, a coherent CSK communications system has been fully examined under a noisy environment with multiple users. As explained in Chapter 1, it is not easy to synchronize the chaotic signals between the transmitters and receivers. Differential CSK (DCSK) has been proposed recently [Kenn 98b], [Kenn 98c], [Kenn 99], [Kis 98a] that allows noncoherent detection with a fixed threshold of zero. In this chapter, we shall first review the operations of a single-user DCSK system. Then, a multiple access technique for use with DCSK (MA-DCSK) is proposed and analysed. Numerical derivations of the bit error probabilities (BEPs), similar to those of CSK, will be performed. Finally, simulations are performed to verify the numerical values.

5.1 Single-User DCSK Communications System

In this section, the basic operation of DCSK under a noiseless environment is reviewed. The transmitter of a DCSK modulator in Figure 3-14 is shown again in Figure 5-1. Assume that the chaotic series $\{x_n\}$ is generated by the map $x_{n+1} = g(x_n)$. In DCSK, every transmitted symbol is represented by two chaotic signal samples. The first one serves as the reference (reference sample) while the second one carries the data (data sample). If a "+1" is to be transmitted, the data sample will be identical to the

reference sample, and if a "−1" is to be transmitted, an inverted version of the reference sample will be used as the data sample. Assume the system starts at $t = 0$ and the binary data to be transmitted has a period of T_b. Denote the transmitted data by $\{d_1, d_2, d_3, ...\} \in \{-1, +1\}$. Let 2α be the spreading factor, defined as T_b/T_c, where α is an integer. Using the aforementioned arrangement, the reference sample for the mth bit is given by

$$\text{ref}^m(t) = \sum_{k=0}^{\alpha-1} x_{k+(m-1)\alpha} r[t - (kT_c + (m-1)T_b)] \tag{5-1}$$

where $r(t)$ is a rectangular pulse of unit amplitude and width T_c, i.e.,

$$r(t) = \begin{cases} 1 & 0 \le t < T_c \\ 0 & \text{elsewhere.} \end{cases} \tag{5-2}$$

The corresponding data sample is

$$\text{data}^m(t) = d_m \text{ref}^m(t - \frac{T_b}{2}). \tag{5-3}$$

The overall transmitted waveform is

$$s(t) = \sum_{m=1}^{\infty} [\text{ref}^m(t) + \text{data}^m(t)]. \tag{5-4}$$

Figure 5-2 shows a typical waveform of $s(t)$ for a spreading factor of 10.

At the receiving end, the reference sample and the corresponding data sample are correlated. Figure 5-3 shows the block diagram of a DCSK correlator receiver. Assume that the channel is perfect and it causes no distortion on the transmitted signal. For the mth transmitted symbol, the output of the correlator at the end of the mth period under a noise-free environment is given by

$$
\begin{aligned}
z(mT_b) &= \int_{(m-1/2)T_b}^{mT_b} p(t)p(t-\frac{T_b}{2})dt \\
&= \int_{(m-1/2)T_b}^{mT_b} s(t)s(t-\frac{T_b}{2})dt \\
&= \int_{(m-1/2)T_b}^{mT_b} \text{data}^m(t)\text{ref}^m(t-\frac{T_b}{2})dt \\
&= \int_{(m-1/2)T_b}^{mT_b} [d_m \text{ref}^m(t-\frac{T_b}{2})]\text{ref}^m(t-\frac{T_b}{2})dt \\
&= d_m \int_{(m-1/2)T_b}^{mT_b} \left(\sum_{k=0}^{\alpha-1} x_{k+(m-1)\alpha} r[t-\frac{T_b}{2}-(kT_c+(m-1)T_b)] \right)^2 dt \\
&= d_m T_c \sum_{k=0}^{\alpha-1} x_{k+(m-1)\alpha}^2 .
\end{aligned}
\tag{5-5}
$$

Depending on whether the output is larger or smaller than the threshold zero, a "+1" or "−1" is decoded. Due to the non-periodic nature of the chaotic signal, $T_c \sum_{k=0}^{\alpha-1} x_{k+(m-1)\alpha}^2$ has a non-zero variance. Hence, $z(mT_b)$ is not constant even when the same symbol is being transmitted repeatedly. Figure 5-4 shows a typical output waveform of the correlator, which is sampled at multiples of T_b. In the presence of noise, the output becomes

$$
\begin{aligned}
z_{\text{noise}}(mT_b) &= \int_{(m-1/2)T_b}^{mT_b} p(t)p(t-\frac{T_b}{2})dt \\
&= \int_{(m-1/2)T_b}^{mT_b} [s(t)+n(t)][s(t-\frac{T_b}{2})+n(t-\frac{T_b}{2})]dt \\
&= \int_{(m-1/2)T_b}^{mT_b} [\text{data}^m(t)+n(t)][\text{ref}^m(t-\frac{T_b}{2})+n(t-\frac{T_b}{2})]dt \\
&= \int_{(m-1/2)T_b}^{mT_b} [d_m\text{ref}^m(t-\frac{T_b}{2})+n(t)][\text{ref}^m(t-\frac{T_b}{2})+n(t-\frac{T_b}{2})]dt \\
&= d_m T_c \sum_{k=0}^{\alpha-1} x_{k+(m-1)\alpha}^2 + d_m \int_{(m-1/2)T_b}^{mT_b} \text{ref}^m(t-\frac{T_b}{2})n(t-\frac{T_b}{2})dt \\
&+ \int_{(m-1/2)T_b}^{mT_b} n(t)\text{ref}^m(t-\frac{T_b}{2})dt + \int_{(m-1/2)T_b}^{mT_b} n(t)n(t-\frac{T_b}{2})dt
\end{aligned}
\tag{5-6}
$$

where $n(t)$ is the noise signal at the input of the receiver. Obviously, since the mean values of the integral terms are all zero, to optimize the BEP, the threshold of the detector should be set at zero. Hence, the threshold of the detector is independent of the noise level.

5.2 Multi-User DCSK Communications System

Suppose there are N users within the system. The chaotic series $\{x_{i,n}\}$ (i = 1, 2, .., N) of the users are generated by the same map $x_{i,n+1} = g(x_{i,n})$. On the other hand, all users are assigned different initial conditions such that different chaotic samples are generated. As explained in the previous section, in a DCSK system with only one user, the reference sample will be transmitted during the first half-bit period and the data sample on the second half-bit period. In a multiple access system, to avoid excessive

interference and hence mis-detection, the separation between the reference and data samples must be different for different users.

Here, we propose a multiple access scheme where the separation between the reference and data samples differs for different users, as illustrated in Figure 5-5. For user i, each data frame will consist of $2i$ half-bit slots. The first i half-bit slots in each frame (slots 1 to i) will be used to transmit the i reference samples while the remaining i half-bit slots (slots i+1 to $2i$) are used to transmit the data samples. If a "+1" is to be transmitted in slot i+1, the sample in slot 1 is repeated in slot i+1, otherwise, an inverted copy is sent. Similarly, in slot i+2, the same or inverted copy of the sample in slot 2 is sent, and so on. As a result, the reference and data samples of user i will be separated by i half-bit periods. Figure 5-6 shows a typical transmitted waveform for user 3.

Let $y_{i,m,f}(t)$ be the reference sample at the mth half-bit slot ($1 \le m \le i$) of the fth data frame for the ith user, i.e., the reference sample at the $[2i(f-1)+m]$th half-bit slot for the ith user. Thus we have

$$y_{i,m,f}(t) = \sum_{k=0}^{\alpha-1} x_{i,k+\alpha[(m-1)+(f-1)i]} r[t-(kT_c+(m-1)\frac{T_b}{2}+(f-1)iT_b)] \tag{5-7}$$

from which we can write the reference samples of user i as

$$\mathrm{ref}_i(t) = \sum_{f=1}^{\infty}\sum_{m=1}^{i} y_{i,m,f}(t). \tag{5-8}$$

Denoting the transmitted data of user i by $\{d_{i,1}, d_{i,2}, d_{i,3}, \ldots\} \in \{-1,+1\}$, the corresponding data samples are given by

$$\mathrm{data}_i(t) = \sum_{f=1}^{\infty}\sum_{m=1}^{i} d_{i,m+(f-1)i}\, y_{i,m,f}(t-\frac{iT_b}{2}) \tag{5-9}$$

and $d_{i,m+(f-1)i}\, y_{i,m,f}(t-\frac{iT_b}{2})$ is the transmitted data sample during the $[2i(f-1)+i+m]$th half-bit slot. Combining the reference and data samples, we obtain the transmitted waveform of the ith user as

$$s_i(t) = \mathrm{ref}_i(t) + \mathrm{data}_i(t) = \sum_{f=1}^{\infty}\sum_{m=1}^{i}[y_{i,m,f}(t) + d_{i,m+(f-1)i}\, y_{i,m,f}(t-\frac{iT_b}{2})]. \tag{5-10}$$

The overall transmitted signal of the whole system is derived by summing the signals of all individual users, i.e., $s(t) = \sum_{i=1}^{N} s_i(t)$.

Figure 5-7 shows the transmitter of a multi-user DCSK system and the receiver of user i. At the receiving end, the half-bit slots in the first half of each frame will correlate with those in the second half. During the same time, the correlator output is sampled every $T_b/2$ before the correlator is reset. The output is then compared with the threshold zero to determine whether a "+1" or "−1" has been received. Figure 5-8 depicts the correlator output and the decoded symbols of user 3 in a 5-user system, assuming a spreading factor of 2000. If the correlation between different samples from the same user or samples from different users is low, a low BEP is expected.

5.2.1 Numerical Analysis

As derived in the previous section, the overall transmitted signal is given by $s(t) = \sum_{i=1}^{N} s_i(t)$. Ignoring the effect of noise and assuming the channel is distortionless, the same signal will arrive at the receiver input. Consider the m_ith reference half-bit slot in the f_ith data frame of the ith user, i.e., the $[2(f_i-1)i+m_i]$th half-bit, where $1 \le m_i \le i$. At

the receiving end, the signal in this half-bit slot will correlate with that in the $[2(f_i-1)i+i+m_i]$th half-bit slot. The output of the correlator is given by

$$z_i(f_i,m_i)=\sum_{u=1}^{N}\sum_{v=1}^{N}\int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} s_u(t)s_v(t-\frac{iT_b}{2})dt \tag{5-11}$$

where $s_u(t)$ and $s_v(t)$ denote the signals of users u and v respectively. For brevity, we define $X_{i,u,v}(f_i,m_i)$ as

$$X_{i,u,v}(f_i,m_i)=\int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} s_u(t)s_v(t-\frac{iT_b}{2})dt\,. \tag{5-12}$$

Hence, $z_i(f_i,m_i)$ can be written as

$$z_i(f_i,m_i)=\sum_{u=1}^{N}\sum_{v=1}^{N}X_{i,u,v}(f_i,m_i). \tag{5-13}$$

For a given binary symbol transmitted for user i, if the $X_{i,u,v}$'s are all independent normal random variables, $z_i(f_i,m_i)$, being the sum of these variables, is also normal with its mean and variance derived as follows.

$$\begin{aligned}\overline{z_i(f_i,m_i)}&=\overline{\sum_{u=1}^{N}\sum_{v=1}^{N}X_{i,u,v}(f_i,m_i)}\\&=\sum_{u=1}^{N}\sum_{v=1}^{N}\overline{X_{i,u,v}(f_i,m_i)}\\&=\overline{X_{i,i,i}(f_i,m_i)}+\sum_{\substack{u=1\\u\neq i}}^{N}\overline{X_{i,u,u}(f_i,m_i)}+\sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N}\overline{X_{i,u,v}(f_i,m_i)}\end{aligned} \tag{5-14}$$

$$\begin{aligned}\mathrm{var}[z_i(f_i,m_i)] &= \mathrm{var}[\sum_{u=1}^{N}\sum_{v=1}^{N} X_{i,u,v}(f_i,m_i)] \\ &= \sum_{u=1}^{N}\sum_{v=1}^{N} \mathrm{var}[X_{i,u,v}(f_i,m_i)] \\ &= \mathrm{var}[X_{i,i,i}(f_i,m_i)] + \sum_{\substack{u=1\\u\neq i}}^{N} \mathrm{var}[X_{i,u,u}(f_i,m_i)] \\ &+ \sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N} \mathrm{var}[X_{i,u,v}(f_i,m_i)]\end{aligned} \tag{5-15}$$

In the sequel, we assume that the cubic map $x_{i,n+1} = g(x_{i,n}) = 4x_{i,n}^3 - 3x_{i,n}$ (i = 1, 2, .., N) is used to generate the chaotic coefficients for user i. It can be readily shown that with this choice of $g(.)$, the $X_{i,u,v}$'s are all normal random variables for a given transmitted binary symbol (see Appendix F). The means and variances of the variables are tabulated in Table 5-1 for spreading factors 2α = 200 and 2000.

Suppose that the $[(f_i-1)i+m_i]$th transmitted symbol of user i is "+1", i.e., $d_{i,(f_i-1)i+m_i} = +1$. Therefore, assuming that the $X_{i,u,v}$'s are also independent, we have

$$\begin{aligned}\overline{z_{i,+1}(f_i,m_i)} &= \overline{X_{i,i,i,+1}(f_i,m_i)} + \sum_{\substack{u=1\\u\neq i}}^{N} \overline{X_{i,u,u}(f_i,m_i)} + \sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N} \overline{X_{i,u,v}(f_i,m_i)} \\ &= 0.25T_b + \sum_{\substack{u=1\\u\neq i}}^{N}(0) + \sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N}(0) \\ &= 0.25T_b\end{aligned} \tag{5-16}$$

and

$$\mathrm{var}[z_{i,+1}(f_i,m_i)]$$

$$= \begin{cases} 0.31\mathrm{x}10^{-3}T_b^2 + \sum_{\substack{u=1\\u\neq i}}^{N} 0.625\mathrm{x}10^{-3}T_b^2 + \sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N} 0.625\mathrm{x}10^{-3}T_b^2 & \alpha = 100 \\ 0.31\mathrm{x}10^{-4}T_b^2 + \sum_{\substack{u=1\\u\neq i}}^{N} 0.625\mathrm{x}10^{-4}T_b^2 + \sum_{\substack{u=1\\u\neq v}}^{N}\sum_{v=1}^{N} 0.625\mathrm{x}10^{-4}T_b^2 & \alpha = 1000 \end{cases} \tag{5-17}$$

$$= \begin{cases} [0.31\mathrm{x}10^{-3} + (N^2-1)0.625\mathrm{x}10^{-3}]T_b^2 & \alpha = 100 \\ [0.31\mathrm{x}10^{-4} + (N^2-1)0.625\mathrm{x}10^{-4}]T_b^2 & \alpha = 1000. \end{cases}$$

The correlator output $z_i(f_i,m_i)$ is then compared with the threshold zero to determine whether a "+1" or "−1" has been received. Since $z_{i,+1}(f_i,m_i)$ is normally distributed, the conditional bit error probability is obtained by

$\mathrm{BEP}_{+1} = \mathrm{Prob}(\, z_i(f_i,m_i) < 0 \mid$ "+1" is transmitted)

$= \mathrm{Prob}(\, z_{i,+1}(f_i,m_i) < 0)$

$$= Q\left(\frac{\overline{z_{i,+1}(f_i,m_i)}}{\sqrt{\mathrm{var}[z_{i,+1}(f_i,m_i)]}} \right). \tag{5-18}$$

Similarly, it can be readily shown that given a "−1" has been transmitted, the correlator output $z_i(f_i,m_i)$ follows a normal distribution with mean

$$\overline{z_{i,-1}(f_i,m_i)} = -0.25T_b \tag{5-19}$$

and variance

$$\mathrm{var}[z_{i,-1}(f_i,m_i)]$$

$$= \begin{cases} [0.31\mathrm{x}10^{-3} + (N^2-1)0.625\mathrm{x}10^{-3}]T_b^2 & \alpha = 100 \\ [0.31\mathrm{x}10^{-4} + (N^2-1)0.625\mathrm{x}10^{-4}]T_b^2 & \alpha = 1000. \end{cases} \tag{5-20}$$

The conditional BEP is now given by

$$\text{BEP}_{-1} = \text{Prob}(z_i(f_i, m_i) > 0 \mid \text{“}-1\text{” is transmitted})$$

$$= \text{Prob}(z_{i,-1}(f_i, m_i) > 0)$$

$$= Q\left(\frac{-\overline{z_{i,-1}(f_i, m_i)}}{\sqrt{\text{var}[z_{i,-1}(f_i, m_i)]}}\right). \tag{5-21}$$

From the equations (5-16) to (5-21), the BEP of user i is derived from

$$\text{BEP} = \text{Prob}(z_i(f_i, m_i) < 0 \mid \text{“}+1\text{” is transmitted})P^+$$

$$+ \text{Prob}(z_i(f_i, m_i) > 0 \mid \text{“}-1\text{” is transmitted})P^-$$

$$= Q\left(\frac{\overline{z_{i,+1}(f_i, m_i)}}{\sqrt{\text{var}[z_{i,+1}(f_i, m_i)]}}\right)P^+ + Q\left(\frac{-\overline{z_{i,-1}(f_i, m_i)}}{\sqrt{\text{var}[z_{i,-1}(f_i, m_i)]}}\right)P^-$$

$$= Q\left(\frac{\overline{z(f_i, m_i)}}{\sqrt{\text{var}[z(f_i, m_i)]}}\right)(P^+ + P^-) \tag{5-22}$$

$$= Q\left(\frac{\overline{z(f_i, m_i)}}{\sqrt{\text{var}[z(f_i, m_i)]}}\right)$$

where

$$\overline{z(f_i, m_i)} = 0.25T_b, \tag{5-23}$$

$$\text{var}[z(f_i, m_i)] = \begin{cases} [0.31\text{x}10^{-3} + (N^2 - 1)0.625\text{x}10^{-3}]T_b^2 & \alpha = 100 \\ [0.31\text{x}10^{-4} + (N^2 - 1)0.625\text{x}10^{-4}]T_b^2 & \alpha = 1000, \end{cases} \tag{5-24}$$

P^+ is the probability of a “+1” being transmitted and P^- is the probability of a “−1” being transmitted. Note that $P^+ + P^- = 1$.

It can be observed from equation (5-24) that the variance of the correlator output increases with N^2. Hence, the performance of the system will degrade quite rapidly with the number of users. Using T_b=10^{-4}s, the BEPs are computed using equation (5-22) for a

range of users with spreading factors 200 and 2000. The results are tabulated in Table 5-2. With an increasing number of users transmitting their chaotic signals at the same time, more interference will be introduced into the system which will cause more errors. Therefore, as shown in the table, the BEP increases with an increasing number of users. For a larger spreading factor, a lower BEP is achieved because of lower correlation between signals from different users.

5.2.2 Simulations

Simulations have been carried out to confirm the feasibility of the proposed multiple access scheme and to verify the foregoing numerical analysis. Spreading factors 200 and 2000 are used and the bit duration T_b is taken as 10^{-4}s. The number of users in the system is assigned up to 50 and different initial conditions are assigned to different users to generate the chaotic signals. 10,000 bits are first sent from each user. Then, the number of errors received by each user and the average number of errors among all users are noted. Table 5-3 shows some typical results obtained. In this example, there are 10 users in the system. It can be observed that all users receive similar number of errors. In other words, the scheme achieves unbiased error probabilities for all users. Table 5-4 shows the average BEPs among all users. As shown in the table, the BEP increases with the number of users but diminishes when the spreading factor is increased from 200 to 2000.

5.2.3 Comparisons

Figure 5-9 compares the numerical BEPs with the simulation results. It can be observed that the simulation results are very close to the numerical ones. As mentioned in Section 5.2.1, the variance of the correlator output increases with N^2. Hence, the BEP becomes high when the number of users is large. On the other hand, by using a higher spreading factor and hence lower autocorrelation and cross-corrrelation values, the system performance can be drastically improved.

5.3 Conclusions

In this chapter, we have proposed a simple multiple access scheme for use with differential chaos shift keying (MA-DCSK). The access scheme of different users is described and the corresponding noncoherent receiver is also designed to decode the signals. The scheme can theoretically be scaled to any number of users, provided the low-correlation property is maintained among the chaotic signal samples representing the different users. As would be expected, the proposed scheme achieves unbiased error probabilities for all users and the error performance degrades as the number of users increases. However, the spreading factor can be increased to improve performance.

In order to evaluate the performance of the system, a simple 1-dimensional iterative cubic map has been used to generate the chaotic signals for all N users. For this particular choice of chaotic generators, it is found that the correlator output follows a normal distribution with variance increases with N^2. The numerical bit error probability (BEP) of the system is also derived. Simulations are then carried out and the results are very close to the numerical BEPs. It is observed that by using chaos generators with a higher spreading factor and hence lower autocorrelation and cross-corrrelation values, the BEPs can be reduced.

Finally, noise appears in any communications systems. It is therefore of interest to study the effect of noise in the MA-DCSK system and to derive similar numerical solutions.

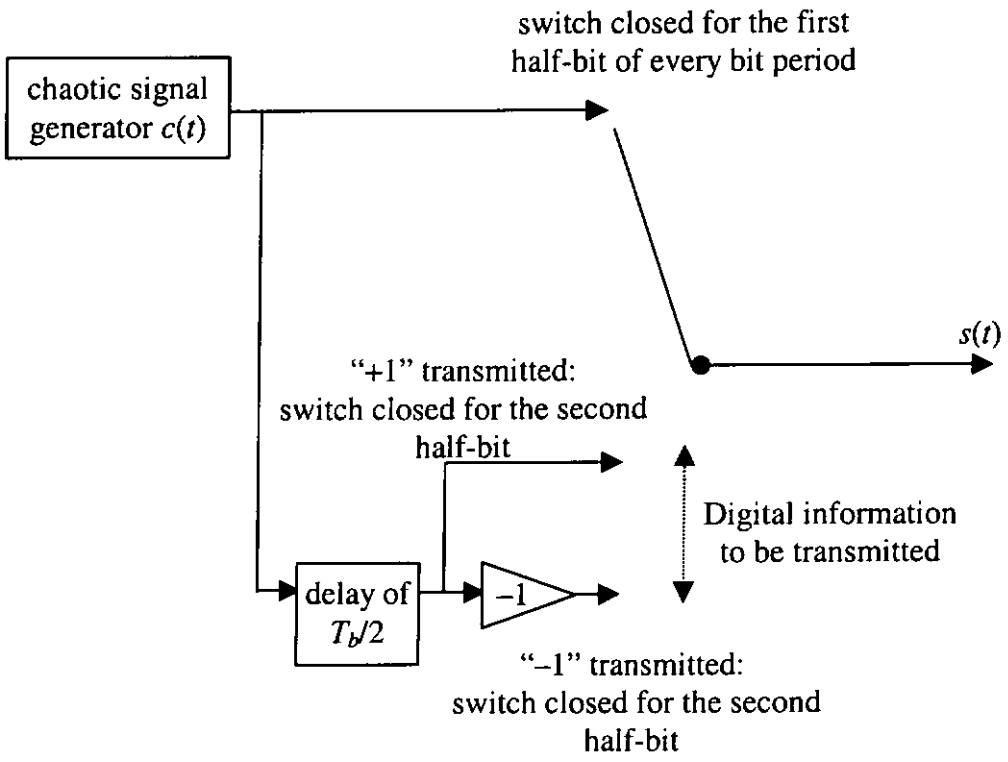


Figure 5-1 Transmitter of a DCSK modulator

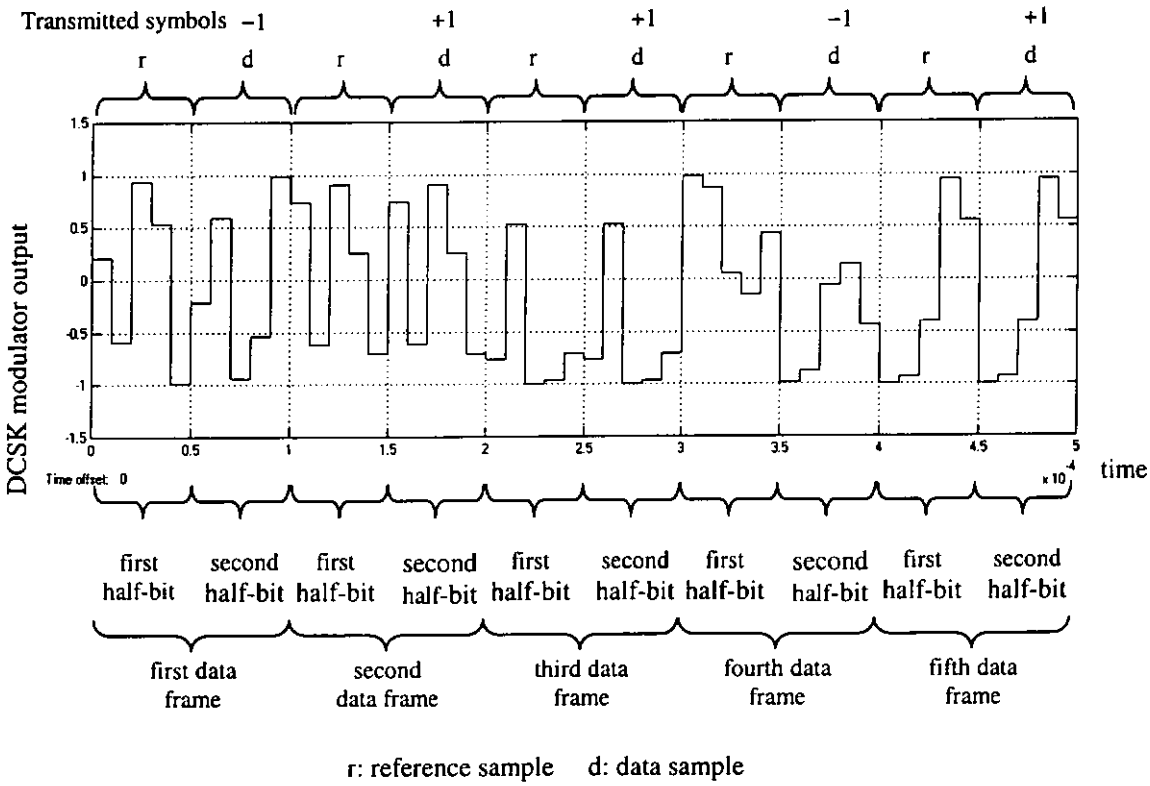


Figure 5-2 A typical DCSK signal

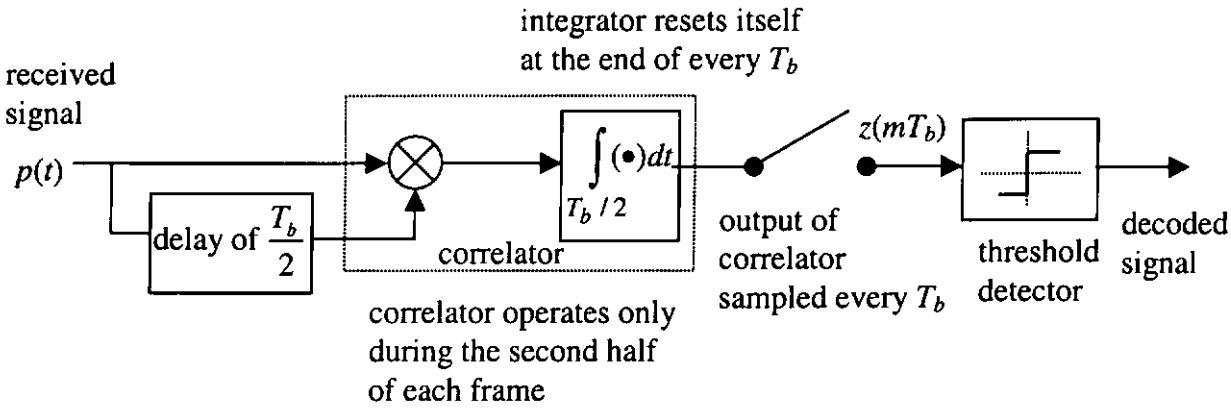


Figure 5-3 Block diagram of a DCSK correlator receiver

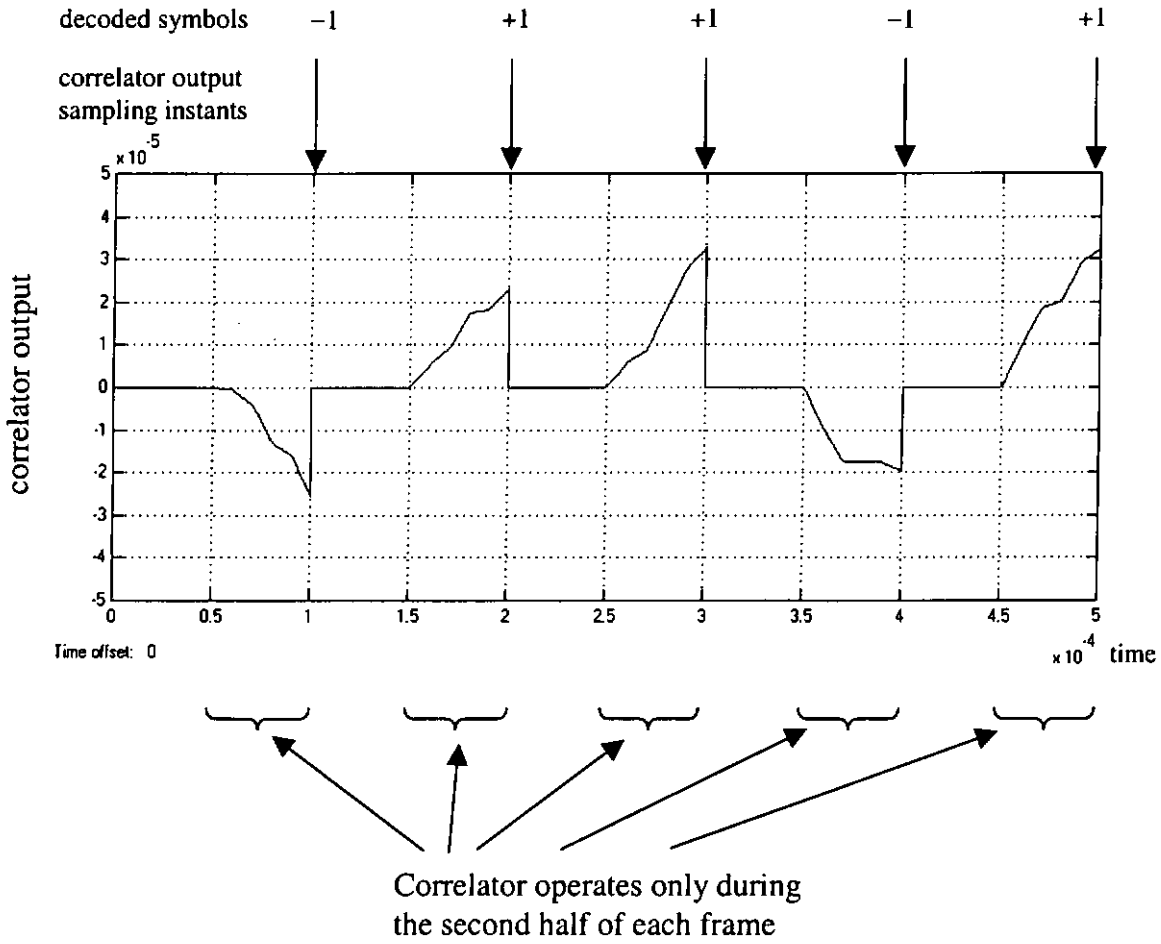


Figure 5-4 Output of the correlator and the decoded symbols in a DCSK receiver

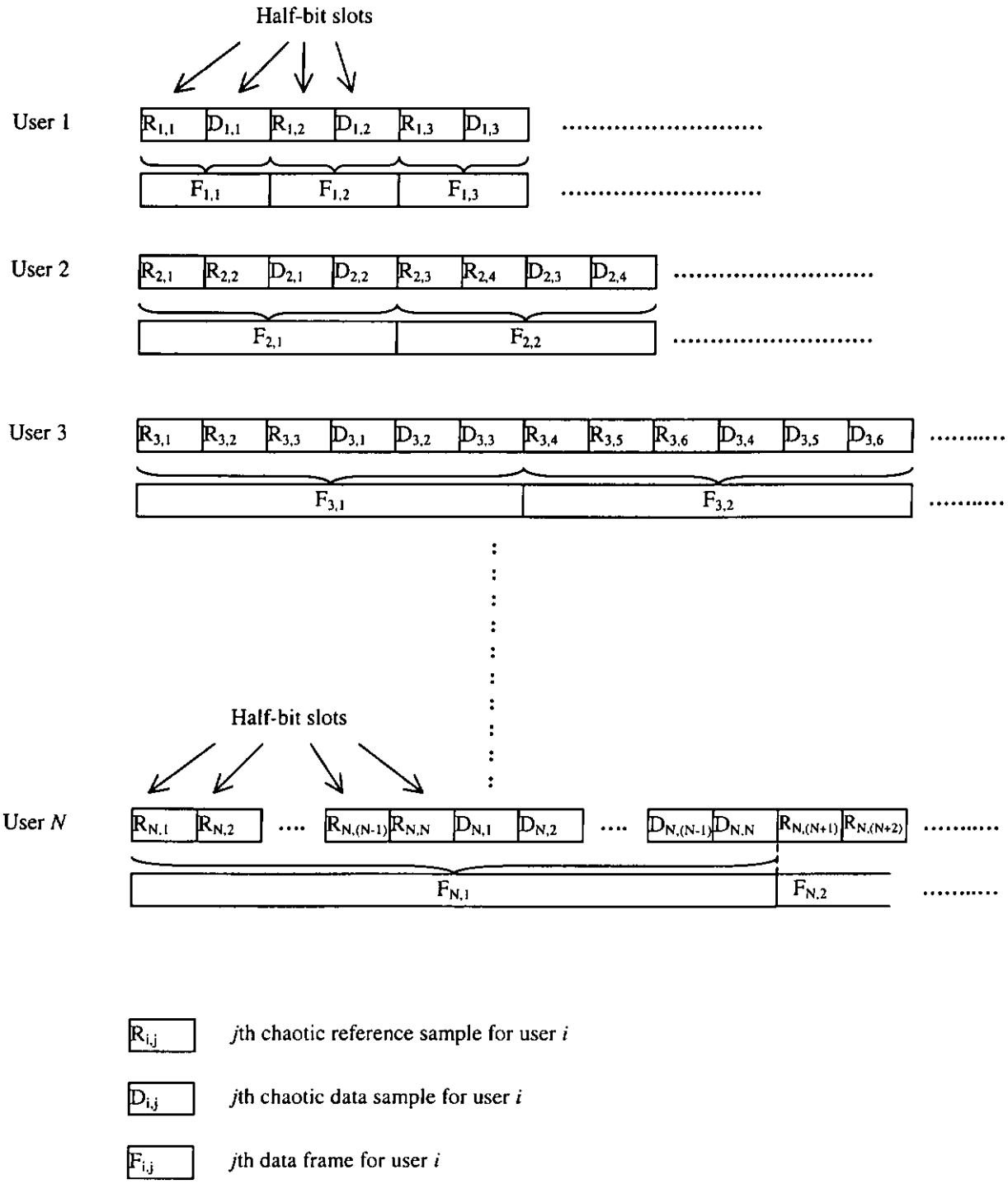


Figure 5-5 Transmission scheme in a multiple access differential chaos shift keying (MA-DCSK) system

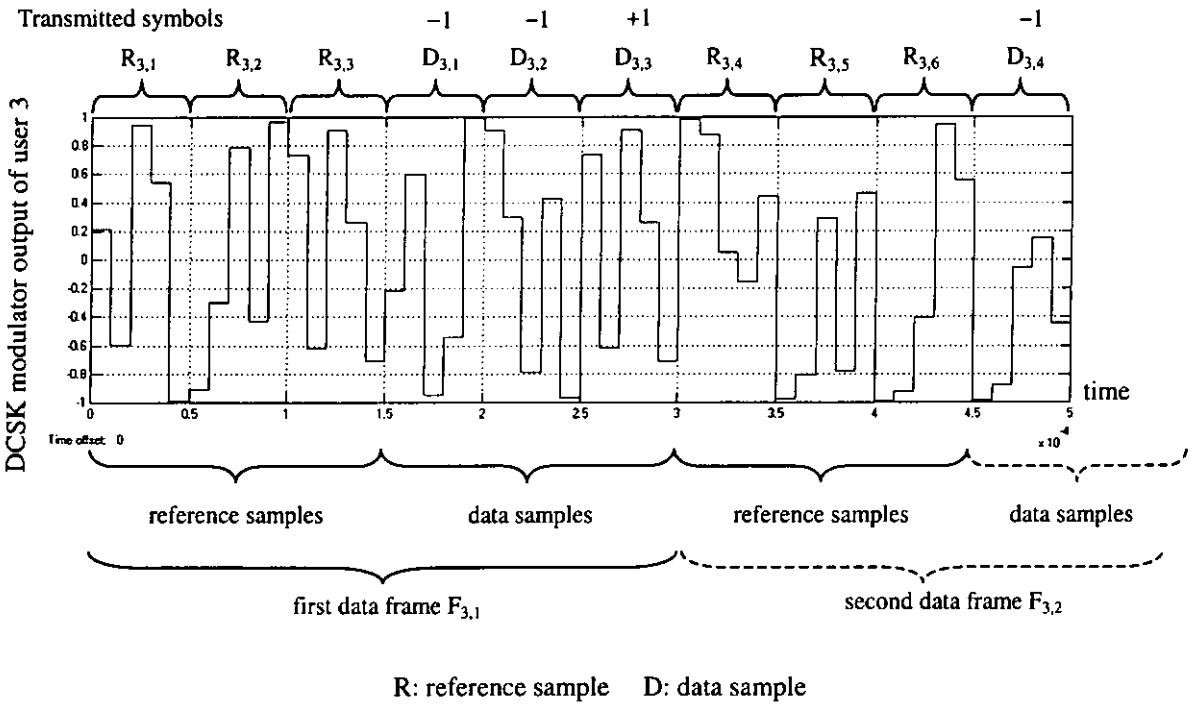


Figure 5-6 A typical transmitted signal for user 3 in a multiple access DCSK system (spreading factor = 10)

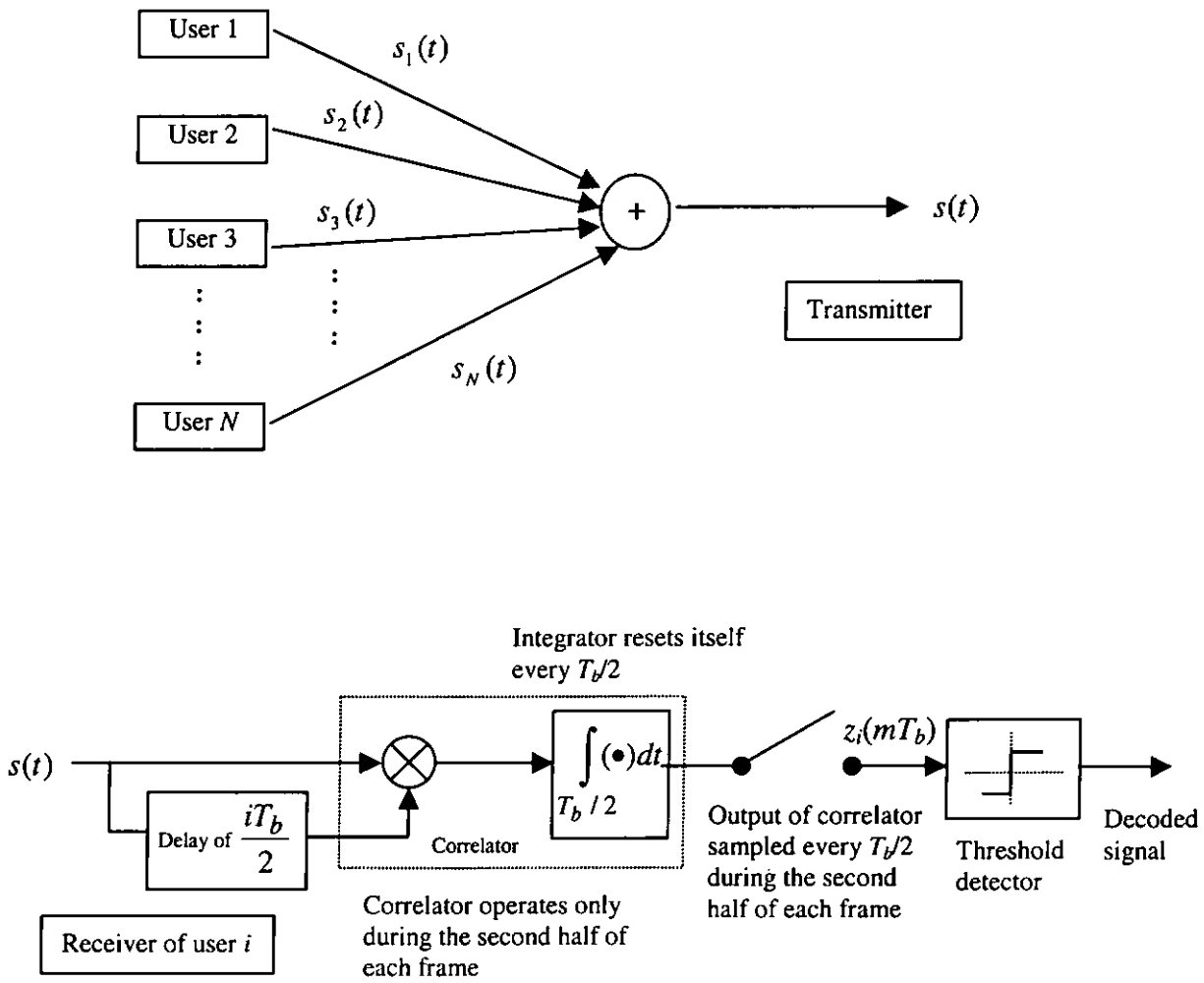


Figure 5-7 Multi-user DCSK transmitter and receiver

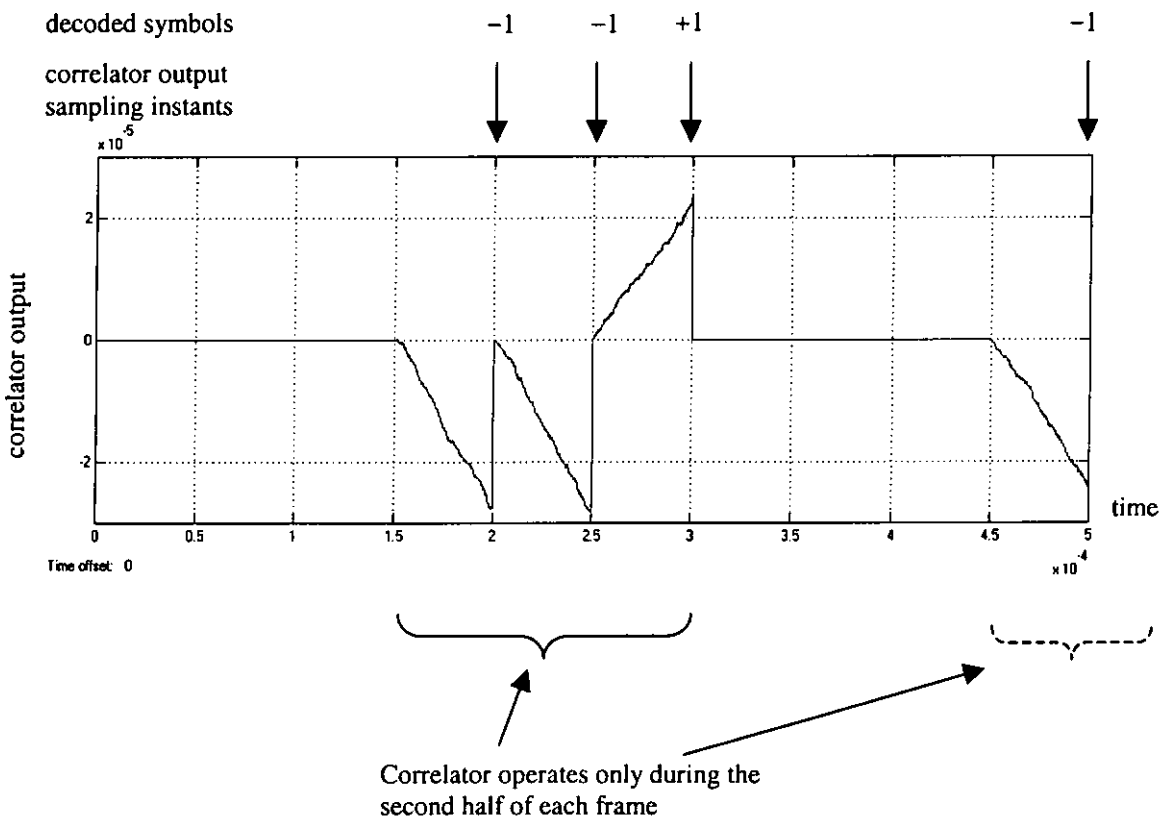


Figure 5-8 Output of the correlator and the decoded symbols of user 3 in a 5-user MA-DCSK system (spreading factor =2000)

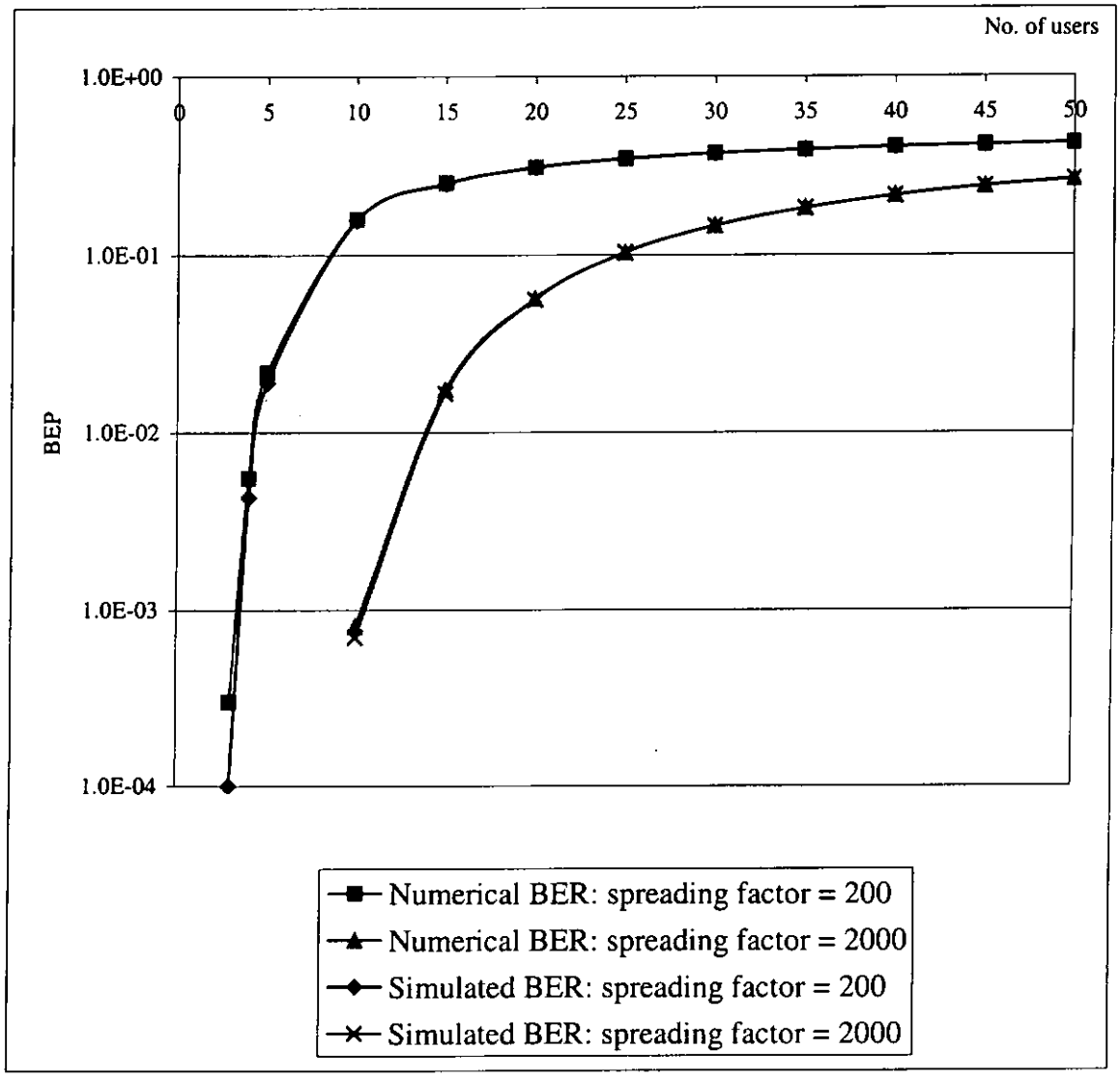


Figure 5-9 Numerical and simulated bit error probabilities against number of users in a multi-user DCSK system

Spreading factor 2α	Statistical properties	Case I: $u = v = i$	Case II: $u = v$, $u \neq i$	Case III: $u \neq v$
200	Mean	$\overline{X_{i,i,i}(f_i, m_i)} = \begin{cases} 0.25T_b & \text{"+1" is transmitted} \\ -0.25T_b & \text{"−1" is transmitted} \end{cases}$	$\overline{X_{i,u,u}(f_i, m_i)} = 0$	$\overline{X_{i,u,v}(f_i, m_i)} = 0$
	Variance	$\mathrm{var}[X_{i,i,i}(f_i, m_i)] = 0.31\mathrm{x}10^{-3} T_b^2$	$\mathrm{var}[X_{i,u,u}(f_i, m_i)] = 0.625\mathrm{x}10^{-3} T_b^2$	$\mathrm{var}[X_{i,u,v}(f_i, m_i)] = 0.625\mathrm{x}10^{-3} T_b^2$
2000	Mean	$\overline{X_{i,i,i}(f_i, m_i)} = \begin{cases} 0.25T_b & \text{"+1" is transmitted} \\ -0.25T_b & \text{"−1" is transmitted} \end{cases}$	$\overline{X_{i,u,u}(f_i, m_i)} = 0$	$\overline{X_{i,u,v}(f_i, m_i)} = 0$
	Variance	$\mathrm{var}[X_{i,i,i}(f_i, m_i)] = 0.31\mathrm{x}10^{-4} T_b^2$	$\mathrm{var}[X_{i,u,u}(f_i, m_i)] = 0.625\mathrm{x}10^{-4} T_b^2$	$\mathrm{var}[X_{i,u,v}(f_i, m_i)] = 0.625\mathrm{x}10^{-4} T_b^2$

Table 5-1 Statistical properties of $X_{i,u,v}(f_i, m_i)$ for spreading factors 200 and 2000

Number of users	Spreading factor 2α	
	200	**2000**
1	0.0000	0.0000
2	0.0000	0.0000
3	0.0003	0.0000
4	0.0055	0.0000
5	0.0217	0.0000
10	0.1580	0.0008
15	0.2523	0.0174
20	0.3084	0.0568
25	0.3445	0.1029
30	0.3694	0.1459
35	0.3875	0.1831
40	0.4013	0.2146
45	0.4121	0.2411
50	0.4207	0.2635

Table 5-2 Numerical bit error probabilities of a multi-user DCSK system

User number	Spreading factor = 200	Spreading factor = 2000
1	1602	11
2	1588	9
3	1564	7
4	1605	7
5	1512	3
6	1562	8
7	1524	4
8	1548	3
9	1591	5
10	1527	11
Average number of errors	1562.3	6.8

Table 5-3 Number of errors received by different users in a 10-user DCSK multiple access system

Number of users	Spreading factor 2α	
	200	**2000**
1	0.0000	0.0000
2	0.0000	0.0000
3	0.0001	0.0000
4	0.0043	0.0000
5	0.0190	0.0000
10	0.1562	0.0007
15	0.2501	0.0166
20	0.3090	0.0560
25	0.3453	0.1031
30	0.3694	0.1453
35	0.3878	0.1825
40	0.4022	0.2152
45	0.4125	0.2418
50	0.4216	0.2653

Table 5-4 Simulated bit error probabilities of a multi-user DCSK system

CHAPTER 6

CRITICAL REVIEW

In this thesis, we have examined the performances of two chaos-based digital communications schemes, namely chaos shift keying (CSK) and differential CSK (DCSK), under a multi-user environment. All simulations and numerical results are generated based on the assumption that a particular cubic map has been used to create the chaotic series. In general, different maps can be used to create chaos for different users. It is also possible to apply another map, different from the cubic map used in this thesis, to multiple users but with different initial conditions. The performance of the system may then be very different. It is expected that chaos with lower partial auto-correlation and cross-correlation values will give better bit error probabilities.

In the coherent detection of CSK, a replica of the chaotic signals are reproduced at the receiver to decode the signal. However, synchronization between chaotic circuits has never been easy. In a multi-user environment where more interference is expected, it is foreseen that synchronization will be very difficult to achieve with only the incoming signal. Under such circumstances, we expect that synchronization will be aided by some other means. For example, if all transmitters and receivers are synchronized with the clock of the global positioning system, a small time drift will be expected between the transmitter and receiver which can be further removed by conventional tracking schemes. As a consequence, a lower synchronization time will be required before bit decoding can commence. On the other hand, if the synchronization

time is comparable with the bit duration, the bit error performance is bound to degrade. Therefore, a fast synchronization scheme will be required to provide a satisfactory bit error performance.

In the thesis, the only defect of the channel is assumed to be additive white Gaussian noise. In a real communications system, the channel allocated to you will have a finite bandwidth. Transmission filter will be added at the transmitter to reduce the signal bandwidth while receiving filter will be used to limit the noise bandwidth at the receiver. More distortion on the signal caused by multipath and fading will be observed in the case of a mobile environment. All such phenomenon will certainly affect the receiving signal drastically. Hence, the system performance should be further investigated under such bandlimited channel and mobile environments. In addition, in conventional spread spectrum communications systems, the received wideband signal, corrupted by wideband noise, is first despread by multiplying it with a replica of the spreading signal at the transmitter. The original narrowband signal is then restored. When the narrowband signal, together with the wideband noise, is passed through another narrowband filter, the noise bandwidth is substantially reduced. As a consequence, the noise power is drastically reduced and the bit error performance is greatly enhanced. Unfortunately, no such despreading process is observed in chaos-based digital communications even when the incoming signals is multiplied with a replica of the chaotic signals. The bandwidth of the signal remains similar. As a result, the noise power can be large. Hence, one way to improve the performances of CSK or DCSK is to try to despread the received signal so as to reduce the signal bandwidth. Then the signal can be passed to a narrowband filter to reduce the noise power and hence improve the bit error performance. Finally, the performance of chaos-based

digital communications systems in the presence of jamming signals should also be studied and compared with that of conventional spread spectrum schemes.

CHAPTER 7

CONCLUSIONS

Chaos communications have received much attention recently because chaotic signals can provide an alternate means to spread the spectrum of signals in digital communications. Unlike other spread spectrum techniques which uses binary codes to spread the spectrum, chaos makes use of its random-like behaviour and wideband nature to carry the binary information. It can provide secured communications with low probability of detection, anti-jamming capability, as well as mitigation of multipath fading.

In this thesis, two chaos-based digital communications schemes have been studied in detail — chaos shifting keying (CSK) and differential chaos shift keying (DCSK). Chaos are assumed to be generated by a simple cubic map. For systems which require more than one chaos sources, the same cubic map with different initial conditions are used.

For CSK, coherent detection is assumed and an analysis on a multi-user system with additive white Gaussian noise has been carried out. Based on the statistical properties of the correlator output, the numerical bit error probabilities (BEPs) of the system are derived which are compared with the simulation results. It is found that the numerical derivation on the BEPs provides a very good estimation of the actual system performance. In general, the BEP decreases with increasing average bit energy to noise

power spectral density ratio ($\overline{E_b} / N_0$). Moreover, the BEPs can be reduced for the same $\overline{E_b} / N_0$ by using a higher spreading ratio. In a multi-user environment, more interference will be introduced into the system when more users are transmitting at the same time. Hence, the interference between users can sometimes pose a lower limit on the BEP. On the other hand, when the performance of the coherent CSK system is compared with a conventional spread spectrum system, results show that the conventional spread spectrum system can achieve a lower BEP. Nevertheless, CSK can provide a more secured communications link because without prior knowledge of the chaotic signals, it is extremely difficult, if not impossible, to synchronize with the noise-like incoming signal and hence decode it.

In this thesis, we have proposed a simple multiple access scheme for use with differential chaos shift keying (MA-DCSK). The access scheme of different users has been shown and the corresponding noncoherent receiver to decode the signals is also constructed. The scheme can theoretically be scaled to any number of users, provided the low-correlation property is maintained among the chaotic signal samples representing the different users. It is found that the correlator output follows a normal distribution with variance increasing with the square of the number of users. Based on this property, the numerical BEP of the system is derived. Simulations are then carried out and the results are consistence with the numerical BEPs. As would be expected, the proposed scheme achieves unbiased error probabilities for all users and the error performance degrades as the number of users increases. However, the spreading factor can be increased to improve performance. It is observed that by using chaos generators

with a higher spreading factor and hence lower autocorrelation and cross-correlation values, the BEP can be reduced.

It should be noted that the multiple access schemes not only apply to the downlink where one base station communicate with many mobile stations in a wireless environment, but also to the reverse link where several mobile stations are transmitting to the same base station. In both cases, similar bit error performances are expected.

At this stage, chaos-based digital modulation schemes are still not as competitive as conventional digital modulation schemes in terms of bit error performances. However, the former schemes do provide fairly high security that the latter ones cannot match. For any unintended users who do not have any prior knowledge of the transmitted chaotic signal, such as the bit rate and the chaos source used, it is extremely difficult to decode the signals. Finally, chaos communications is still a young research area and there are lots of issues to be tackle. Possible topics include the effect of noise in the MA-DCSK system and the effect of the synchronization error and synchronization time in the coherent CSK system.

Appendix A

Partial Discrete Auto-correlation Function

The partial discrete auto-correlation function of the chaotic series $\{x_n\}$ has been defined as

$$\gamma_x(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n}x_{l+n} \tag{A-1}$$

where all symbols have their meanings as defined in the thesis. 10 initial conditions have first been selected. For each of them, more than 10^7 iterations have been performed to generate the chaotic series for the analyses below.

A.1 Case I — *k=l*

For each of the initial conditions, the partial discrete auto-correlation value is first computed for every L iterations performed. After collecting 10,000 values in each case, we analyse the distribution of the values. It is found that in all cases, the auto-correlation value follows a normal distribution. The statistics of the partial discrete auto-correlation function are tabulated in Tables A-1 and A-2. It can be observed that in both cases L=100 and L=1000, the mean value is about 0.5. For the variance, it equals $1.24\text{x}10^{-3}$ and $1.24\text{x}10^{-4}$ respectively for L=100 and L=1000.

A.2 Case II — $k \neq l$

For each of the initial conditions, the first 10 chaotic samples each of length L are first stored in memory. The partial discrete auto-correlation function between each of these reference samples and the next 10,000 samples are computed. The distributions of the values are then analysed. It is found that in all cases, the partial discrete auto-correlation value follows a normal distribution. Two typical statistics of the partial discrete auto-correlation function are tabulated in Tables A-3 and A-4. It can be observed that the distribution of the partial discrete auto-correlation function does not depend much on the mean-squared value of the reference sample. Moreover, in both cases L=100 and L=1000, the mean value of the partial discrete auto-correlation function is nearly zero. For the variance, it equals to 2.5×10^{-3} and 2.5×10^{-4} respectively for L=100 and L=1000.

initial condition number	Partial discrete auto-correlation function			
	maximum	minimum	mean	variance
1	0.6325	0.3628	0.4997	0.00123
2	0.6225	0.3671	0.5001	0.00121
3	0.6241	0.3770	0.4999	0.00124
4	0.6449	0.3054	0.4998	0.00125
5	0.6369	0.3657	0.4997	0.00125
6	0.6282	0.3509	0.4993	0.00127
7	0.6358	0.3602	0.4997	0.00125
8	0.6275	0.3303	0.4996	0.00125
9	0.6219	0.3686	0.5006	0.00123
10	0.6474	0.3792	0.5001	0.00126
		average	0.4999	0.00124

Table A-1 Statistics of the partial discrete auto-correlation function for different initial conditions with $k=l$ and $L=100$

initial condition number	Partial discrete auto-correlation function			
	maximum	minimum	mean	variance
1	0.5433	0.4582	0.4999	0.000125
2	0.5429	0.4584	0.5001	0.000125
3	0.5398	0.4604	0.4998	0.000123
4	0.5399	0.4507	0.5000	0.000123
5	0.5478	0.4524	0.5002	0.000123
6	0.5478	0.4568	0.4997	0.000128
7	0.5470	0.4619	0.5000	0.000125
8	0.5470	0.4518	0.4999	0.000123
9	0.5386	0.4566	0.5002	0.000121
10	0.5381	0.4590	0.5000	0.000123
		average	0.5000	0.000124

Table A-2 Statistics of the partial discrete auto-correlation function for different initial conditions with $k=l$ and $L=1000$

Reference Sample No.	Mean-squared Value of Reference Sample	Partial discrete auto-correlation function			
		maximum	minimum	mean	variance
1	0.5087	0.1868	-0.1958	-0.0004	0.0025
2	0.5585	0.2000	-0.1954	-0.0002	0.0028
3	0.5401	0.1717	-0.1888	-0.0009	0.0027
4	0.5167	0.1790	-0.2090	-0.0002	0.0026
5	0.4575	0.1878	-0.1692	-0.0001	0.0023
6	0.4946	0.1850	-0.2500	0.0004	0.0025
7	0.4831	0.1634	-0.1828	-0.0004	0.0024
8	0.5389	0.1875	-0.1889	0.0002	0.0027
9	0.5058	0.1746	-0.1889	0.0004	0.0026
10	0.4747	0.1933	-0.1851	0.0005	0.0024
			average	-0.0001	0.0025

Table A-3 Typical statistics of the partial discrete auto-correlation function with $k \neq l$ and $L = 100$

Reference Sample No.	Mean-squared Value of Reference Sample	Partial discrete auto-correlation function			
		maximum	minimum	mean	variance
1	0.5079	0.0554	-0.0577	0.0000	0.00024
2	0.5066	0.0566	-0.0621	0.0000	0.00026
3	0.4989	0.0623	-0.0689	0.0000	0.00024
4	0.4812	0.0561	-0.0578	0.0000	0.00025
5	0.4960	0.0548	-0.0628	0.0001	0.00025
6	0.5208	0.0589	-0.0569	0.0001	0.00026
7	0.4857	0.0631	-0.0520	-0.0001	0.00024
8	0.5077	0.0575	-0.0533	0.0001	0.00025
9	0.4997	0.0588	-0.0583	0.0000	0.00024
10	0.4806	0.0585	-0.0666	-0.0001	0.00024
			average	0.0000	0.00025

Table A-4 Typical statistics of the partial discrete auto-correlation function with $k \neq l$ and $L = 1000$

Appendix B

Partial Discrete Cross-correlation Function

The partial discrete cross-correlation function of the chaotic series $\{x_n\}$ has been defined as

$$\gamma_{xx'}(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n} x'_{l+n} \tag{B-1}$$

where all symbols have their meanings as defined in the thesis. 10 initial conditions have first been selected. For each of them, more than 10^7 iterations have been performed to generate the chaotic series for the analysis below.

Using the 10 initial conditions, 10 chaotic sample sets (#1 To #10), each consists of 10,000 chaotic samples of length L, are computed. For set #1, the first 10 samples are now used as references. The partial discrete cross-correlation functions between each of the reference samples and each of the other 9 chaotic sample sets are computed. The procedure is repeated for sets #2, #3, etc.. The distributions of the partial discrete cross-correlation functions are then analysed. Four typical results are shown in Tables B-1 and B-2. It can be observed that the distribution of the cross-correlation function does not depend on the mean-squared value of the reference sample. Summarizing all the results obtained, it is found that in both cases L=100 and L=1000, the mean value of the partial discrete cross-correlation function is nearly zero. For the variance, it equals to $2.5\text{x}10^{-3}$ and $2.5\text{x}10^{-4}$ respectively for L=100 and L=1000.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.5087	0.1697	-0.2019	0.0005	0.0026
2	0.5585	0.2015	-0.2233	0.0005	0.0028
3	0.5401	0.1912	-0.1894	0.0004	0.0027
4	0.5167	0.1819	-0.1873	-0.0010	0.0026
5	0.4575	0.1493	-0.1803	-0.0004	0.0023
6	0.4946	0.1973	-0.1805	-0.0012	0.0025
7	0.4831	0.1891	-0.1848	-0.0002	0.0024
8	0.5389	0.2027	-0.1890	-0.0007	0.0027
9	0.5058	0.1974	-0.1978	-0.0003	0.0025
10	0.4747	0.1877	-0.2217	0.0000	0.0024
			average	-0.0002	0.0025

Table B-1a Typical statistics of the partial discrete cross-correlation function. Reference samples, generated by initial condition #1, correlates with 10,000 samples generated by initial condition #2 with L =100.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.4654	0.1820	-0.1840	0.0004	0.0023
2	0.5154	0.1897	-0.1750	0.0007	0.0026
3	0.4855	0.1716	-0.2025	0.0007	0.0024
4	0.5872	0.2078	-0.2100	-0.0013	0.0029
5	0.5603	0.2456	-0.2104	0.0004	0.0028
6	0.4721	0.2059	-0.1617	0.0000	0.0024
7	0.4781	0.1687	-0.1657	0.0002	0.0024
8	0.5273	0.1963	-0.2110	0.0000	0.0026
9	0.5662	0.2213	-0.2092	0.0002	0.0028
10	0.5472	0.2112	-0.1920	-0.0004	0.0028
			average	0.0001	0.0026

Table B-1b Typical statistics of the partial discrete cross-correlation function. Reference samples, generated by initial condition #2, correlates with 10,000 samples generated by initial condition #3 with L =100.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.5079	0.0624	-0.0577	-0.0002	0.00026
2	0.5066	0.0634	-0.0609	0.0002	0.00025
3	0.4989	0.0627	-0.0666	0.0000	0.00025
4	0.4812	0.0622	-0.0561	-0.0001	0.00024
5	0.4960	0.0598	-0.0556	0.0000	0.00025
6	0.5208	0.0634	-0.0627	-0.0002	0.00026
7	0.4857	0.0568	-0.0600	0.0001	0.00024
8	0.5077	0.0519	-0.0651	-0.0002	0.00025
9	0.4997	0.0732	-0.0586	0.0000	0.00025
10	0.4806	0.0582	-0.0656	0.0001	0.00024
			average	0.0000	0.00025

Table B-2a Typical statistics of the partial discrete cross-correlation function. Reference samples, generated by initial condition #1, correlates with 10,000 samples generated by initial condition #3 with L =1000.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.5205	0.0637	-0.0729	0.0002	0.00025
2	0.5202	0.0716	-0.0647	0.0001	0.00027
3	0.5056	0.0585	-0.0668	0.0001	0.00025
4	0.5071	0.0698	-0.0604	0.0002	0.00026
5	0.4862	0.0647	-0.0597	-0.0002	0.00025
6	0.4957	0.0670	-0.0676	-0.0001	0.00025
7	0.4941	0.0563	-0.0536	-0.0002	0.00026
8	0.5079	0.0656	-0.0671	0.0001	0.00026
9	0.4973	0.0628	-0.0596	0.0002	0.00025
10	0.4951	0.0532	-0.0690	0.0000	0.00025
			average	0.0000	0.00025

Table B-2b Typical statistics of the partial discrete cross-correlation function. Reference samples, generated by initial condition #2, correlates with 10,000 samples generated by initial condition #1 with L =1000.

Appendix C

Partial Discrete Cross-correlation Function between Chaotic Series and Normal Random Sequences

The partial discrete cross-correlation function between a chaotic series $\{x_n\}$ and a normal random sequence $\{\phi_n\}$ is defined as

$$\gamma_{x\phi}(k,l,L) = \frac{1}{L}\sum_{n=0}^{L-1} x_{k+n}\phi_{l+n} \cdot \tag{C-1}$$

The elements of $\{\phi_n\}$ are normal random variables with zero mean and unit variance. Two sets of simulations have been performed. One uses the normal random sequence samples as reference and the other keep the chaotic samples fixed.

C.1 Fixed Normal Random Sequence Samples

100 normal random sequence samples, each of length L, are first generated and used as references. Then, using 10 initial conditions, 10 chaotic sample sets, each consists of 10,000 chaotic samples of length L, are computed. The partial discrete cross-correlation between each of the reference random sequence samples and each of the chaotic sample sets are computed. The distributions of the computed values are then analyzed. Two typical distributions are partially shown in Tables C-1 and C-2. Summarizing all the results obtained, the partial discrete cross-correlation function is

found to have a zero mean and variance of 5.0×10^{-3} and 5.0×10^{-4} for L=100 and L=1000 respectively.

C.2 Fixed Chaotic Sequence Samples

For each of the 10 chaotic series, the first 100 samples, each of length L, are now used as references. 10,000 normal random sequence samples are then generated and correlate with the reference samples. The statistics of the distributions are partially shown in Tables C-3 and C-4. As shown in the tables, the partial discrete cross-correlation function can be modelled as a normal random variable with zero mean and 5.0×10^{-3} and 5.0×10^{-4} for L=100 and L=1000 respectively.

Consolidating the results obtained from the two sets of data above, the partial discrete cross-correlation function between the chaotic series and the normal random sequence can be modelled as a normal random variable with zero mean and variance 5.0×10^{-3} and 5.0×10^{-4} for L=100 and L=1000 respectively.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.8584	0.2551	-0.2744	-0.0008	0.0044
2	0.7402	0.2337	-0.2138	-0.0011	0.0038
3	1.1121	0.2724	-0.2692	-0.0008	0.0055
4	0.8725	0.2515	-0.2754	0.0009	0.0044
5	0.9041	0.2514	-0.2603	0.0011	0.0046
6	1.0404	0.3019	-0.2565	-0.0012	0.0052
7	1.1773	0.3125	-0.3231	0.0004	0.0059
8	1.3788	0.3501	-0.3054	0.0001	0.0070
9	0.9076	0.2376	-0.2392	0.0007	0.0044
10	1.0589	0.2954	-0.2839	-0.0005	0.0052
11	0.9592	0.2455	-0.2639	0.0000	0.0047
12	0.9780	0.2650	-0.2530	0.0010	0.0048
13	1.3833	0.3343	-0.3107	-0.0012	0.0069
14	0.9792	0.2489	-0.2737	-0.0005	0.0049
15	0.8095	0.2205	-0.2571	-0.0006	0.0041
16	0.7632	0.2297	-0.2095	-0.0003	0.0038
:	:	:	:	:	:
85	0.9164	0.2406	-0.2556	-0.0003	0.0046
86	0.8235	0.2597	-0.2294	-0.0001	0.0041
87	0.9836	0.2422	-0.2600	0.0016	0.0049
88	1.0127	0.3399	-0.2749	-0.0010	0.0052
89	0.8840	0.2375	-0.2275	0.0001	0.0044
90	1.0303	0.2606	-0.2865	-0.0004	0.0051
91	1.3347	0.2931	-0.2992	0.0003	0.0065
92	0.9857	0.2228	-0.2610	0.0004	0.0050
93	0.8321	0.2444	-0.2443	0.0003	0.0041
94	0.9090	0.2249	-0.2817	0.0010	0.0046
95	1.2657	0.3212	-0.2767	0.0009	0.0063
96	0.9034	0.2641	-0.2621	0.0005	0.0045
97	0.9881	0.2934	-0.2676	-0.0003	0.0049
98	1.0142	0.2805	-0.2704	-0.0003	0.0050
99	0.8291	0.2483	-0.2418	0.0001	0.0040
100	1.0400	0.2758	-0.2593	0.0006	0.0052
			average	0.0001	0.0050

Table C-1 Typical statistics of the partial discrete cross-correlation function between the chaotic series and normal random sequence. Reference samples are normal random sequence samples. They correlate with 10,000 chaotic samples generated by initial condition #1 with L =100.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.9799	0.0900	-0.1009	-0.0001	0.0005
2	0.9633	0.0846	-0.0879	0.0000	0.0005
3	1.0769	0.0864	-0.0881	0.0002	0.0005
4	1.0575	0.0909	-0.1010	0.0000	0.0005
5	0.9422	0.0702	-0.0873	-0.0002	0.0005
6	0.9889	0.0862	-0.1053	-0.0002	0.0005
7	0.9969	0.0942	-0.0808	0.0001	0.0005
8	1.0893	0.0903	-0.0853	-0.0004	0.0006
9	1.0009	0.0878	-0.0887	0.0001	0.0005
10	1.0006	0.0929	-0.0841	0.0001	0.0005
11	1.0080	0.0967	-0.0779	-0.0002	0.0005
12	1.0453	0.0815	-0.0912	-0.0002	0.0005
13	1.0109	0.0935	-0.0763	-0.0001	0.0005
14	1.0099	0.0773	-0.0799	-0.0001	0.0005
15	0.9814	0.0847	-0.0778	0.0001	0.0005
16	1.0482	0.0913	-0.0934	-0.0003	0.0005
:	:	:	:	:	:
85	0.9686	0.0767	-0.0871	0.0000	0.0005
86	0.9842	0.0775	-0.0824	0.0002	0.0005
87	0.9626	0.0902	-0.0862	0.0002	0.0005
88	0.9769	0.0790	-0.0973	-0.0001	0.0005
89	0.9325	0.0875	-0.0797	0.0007	0.0005
90	0.9823	0.0789	-0.0883	0.0001	0.0005
91	0.9828	0.0931	-0.0750	0.0000	0.0005
92	0.9683	0.0908	-0.0801	0.0001	0.0005
93	0.9998	0.0853	-0.0917	-0.0001	0.0005
94	1.0445	0.0819	-0.0922	0.0000	0.0005
95	0.9985	0.0856	-0.1012	-0.0002	0.0005
96	1.0416	0.0771	-0.0849	0.0001	0.0005
97	1.0308	0.0877	-0.1016	-0.0002	0.0005
98	0.9598	0.0774	-0.0831	-0.0001	0.0005
99	1.0183	0.0789	-0.0824	-0.0003	0.0005
100	0.9934	0.1028	-0.0866	0.0005	0.0005
			average	0.0000	0.0005

Table C-2 Typical statistics of the partial discrete cross-correlation function between the chaotic series and normal random sequence. Reference samples are normal random sequence samples. They correlate with 10,000 chaotic samples generated by initial condition #2 with $L = 1000$.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.5087	0.2417	-0.2634	0.0010	0.0051
2	0.5585	0.2939	-0.2633	-0.0001	0.0056
3	0.5401	0.2863	-0.2952	-0.0013	0.0054
4	0.5167	0.2899	-0.2701	-0.0010	0.0051
5	0.4575	0.2604	-0.2814	0.0002	0.0045
6	0.4946	0.2367	-0.2609	-0.0008	0.0048
7	0.4831	0.2496	-0.2683	0.0008	0.0047
8	0.5389	0.3033	-0.2793	-0.0006	0.0055
9	0.5058	0.2727	-0.2643	-0.0003	0.0051
10	0.4747	0.2796	-0.2690	0.0004	0.0047
11	0.4722	0.2786	-0.2756	-0.0007	0.0046
12	0.5242	0.2480	-0.2653	0.0006	0.0052
13	0.5298	0.2759	-0.3447	-0.0004	0.0053
14	0.5235	0.2670	-0.2391	0.0008	0.0052
15	0.4813	0.2539	-0.2575	0.0007	0.0050
16	0.5305	0.2989	-0.2981	-0.0003	0.0053
:	:	:	:	:	:
985	0.4207	0.2190	-0.2414	-0.0004	0.0041
986	0.4565	0.2870	-0.2706	0.0002	0.0045
987	0.4409	0.2299	-0.2624	-0.0007	0.0043
988	0.5337	0.2798	-0.3451	0.0013	0.0054
989	0.5683	0.2875	-0.2702	-0.0004	0.0056
990	0.4899	0.2489	-0.3002	-0.0010	0.0050
991	0.4850	0.2572	-0.2594	0.0005	0.0050
992	0.4974	0.2576	-0.2551	0.0008	0.0049
993	0.5138	0.2857	-0.3328	-0.0006	0.0050
994	0.4926	0.2743	-0.2389	0.0005	0.0048
995	0.4852	0.2885	-0.2720	-0.0002	0.0048
996	0.4849	0.2588	-0.2797	0.0003	0.0049
997	0.4717	0.2734	-0.2488	0.0001	0.0047
998	0.5631	0.3106	-0.2918	-0.0006	0.0055
999	0.4541	0.2352	-0.2682	0.0002	0.0046
1000	0.5161	0.3034	-0.3038	0.0001	0.0051
			average	0.0000	0.0050

Table C-3 Statistics of the partial discrete cross-correlation function between the chaotic series and normal random sequence. Reference samples are chaotic samples generated by 10 different initial conditions. They correlate with 10,000 normal random sequence samples with L =100.

Reference Sample Number	Mean-squared Value of Reference Sample	Partial discrete cross-correlation function			
		maximum	minimum	mean	variance
1	0.5079	0.0801	-0.0818	-0.0002	0.0005
2	0.5066	0.0922	-0.0796	-0.0001	0.0005
3	0.4989	0.0887	-0.0840	0.0002	0.0005
4	0.4812	0.0902	-0.0800	-0.0001	0.0005
5	0.4960	0.0780	-0.0887	-0.0001	0.0005
6	0.5208	0.0843	-0.0968	0.0000	0.0005
7	0.4857	0.0882	-0.0775	0.0002	0.0005
8	0.5077	0.0814	-0.0837	-0.0001	0.0005
9	0.4997	0.0842	-0.1046	0.0000	0.0005
10	0.4806	0.0847	-0.0891	0.0003	0.0005
11	0.5043	0.0909	-0.0888	0.0000	0.0005
12	0.5004	0.0878	-0.0964	-0.0001	0.0005
13	0.4938	0.0839	-0.0813	-0.0001	0.0005
14	0.4912	0.0930	-0.0870	0.0000	0.0005
15	0.4999	0.0931	-0.0862	0.0000	0.0005
16	0.5137	0.0764	-0.0918	-0.0001	0.0005
:	:	:	:	:	:
985	0.5099	0.0865	-0.0905	0.0000	0.0005
986	0.4982	0.0856	-0.0925	-0.0001	0.0005
987	0.5050	0.0938	-0.0767	0.0002	0.0005
988	0.4803	0.0722	-0.0893	0.0001	0.0005
989	0.5248	0.0923	-0.1036	-0.0001	0.0005
990	0.4900	0.0809	-0.0771	0.0001	0.0005
991	0.4888	0.0769	-0.0829	0.0000	0.0005
992	0.4973	0.0890	-0.0903	0.0000	0.0005
993	0.4977	0.0930	-0.0858	-0.0001	0.0005
994	0.5221	0.0875	-0.0892	0.0000	0.0005
995	0.5020	0.0938	-0.0845	0.0001	0.0005
996	0.4893	0.0812	-0.0827	0.0000	0.0005
997	0.5103	0.0826	-0.0851	-0.0004	0.0005
998	0.4979	0.0780	-0.0847	0.0000	0.0005
999	0.5065	0.0793	-0.0748	0.0004	0.0005
1000	0.4832	0.0914	-0.0919	-0.0002	0.0005
			average	0.0000	0.0005

Table C-4 Statistics of the partial discrete cross-correlation function between the chaotic series and normal random sequence. Reference samples are chaotic samples generated by 10 different initial conditions. They correlate with 10,000 normal random sequence samples with L =1000.

Appendix D

Equivalent Noise Source

In a coherent CSK system corrupted by additive white Gaussian noise (AWGN), the input to the demodulator is given by

$$\begin{aligned} p(t) &= s(t) + n(t) \\ &= \sum_{m=1}^{\infty} v^m(t) + n(t) \end{aligned} \tag{D-1}$$

where $n(t)$ is an AWGN with a two-sided power spectral density of

$$S_n(f) = \frac{N_0}{2} \text{ for all } f. \tag{D-2}$$

For the mth received symbol, the output of the correlator$_{-1}$ at the end of the period is given by

$$\begin{aligned} \text{Corr}_{-1}(mT_b) &= \int_{(m-1)T_b}^{mT_b} p(t)c_{-1}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} [v^m(t) + n(t)]c_{-1}(t)dt \\ &= \int_{(m-1)T_b}^{mT_b} v^m(t)c_{-1}(t)dt + \int_{(m-1)T_b}^{mT_b} n(t)c_{-1}(t)dt. \end{aligned} \tag{D-3}$$

Consider the output component due to noise

$$I_{\text{noise}} = \int_{(m-1)T_b}^{mT_b} n(t)c_{-1}(t)dt. \tag{D-4}$$

It can be divided into several components shown below.

$$
\begin{aligned}
I_{\text{noise}} &= \int_{(m-1)T_b}^{mT_b} n(t)c_{-1}(t)dt \\
&= \int_{(m-1)T_b}^{mT_b} n(t) \sum_{k=(m-1)\beta}^{m\beta-1} x_{-1,k} r(t-kT_c)dt \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} \int_{(m-1)T_b}^{mT_b} n(t)x_{-1,k} r(t-kT_c)dt \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} \int_{kT_c}^{(k+1)T_c} n(t)x_{-1,k} r(t-kT_c)dt \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} x_{-1,k} \int_{kT_c}^{(k+1)T_c} n(t)dt \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} n_k
\end{aligned}
\tag{D-5}
$$

where $n_k = x_{-1,k} \int_{kT_c}^{(k+1)T_c} n(t)dt$. The noise components $\{n_k\}$ are Gaussian. Their mean values are

$$
E[n_k] = x_{-1,k} \int_{kT_c}^{(k+1)T_c} E[n(t)]dt = 0 \tag{D-6}
$$

for all k. Their covariances are

$$
\begin{aligned}
E[n_j n_k] &= x_{-1,j} x_{-1,k} \int_{jT_c}^{(j+1)T_c} \int_{kT_c}^{(k+1)T_c} E[n(t)n(\tau)]d\tau dt \\
&= x_{-1,j} x_{-1,k} \int_{jT_c}^{(j+1)T_c} \int_{kT_c}^{(k+1)T_c} \frac{N_0}{2}\delta(t-\tau)d\tau dt \\
&= x_{-1,j} x_{-1,k} \frac{N_0}{2} \int_{jT_c}^{(j+1)T_c} \int_{kT_c}^{(k+1)T_c} \delta(t-\tau)d\tau dt \\
&= x_{-1,k}^2 \frac{N_0 T_c}{2} \delta_{jk}
\end{aligned}
\tag{D-7}
$$

where $\delta_{jk} = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases}$. Hence, the noise components $\{n_k\}$ are zero mean uncorrelated Gaussian variables with variances $\sigma_{n_k}^2 = x_{-1,k}^2 \frac{N_0 T_c}{2}$. Since the noise components are uncorrelated Gaussian random variables, they are also statistically independent.

Consider another noise source given by

$$
n'(t) = \sum_{k=0}^{\infty} \xi_k r(t - kT_c) \tag{D-8}
$$

where the coefficients $\{\xi_k\}$ are independent Gaussian random variables with mean $\overline{\xi_k}$ and variance $\sigma_{n'}^2$. Replace the AWGN noise source in equation (D-1) by $n'(t)$ and follow the aforementioned procedures, the correlator output component due to the new noise source can be shown to be

$$
\begin{aligned}
I_{\text{noise}}' &= \sum_{k=(m-1)\beta}^{m\beta-1} x_{-1,k} \int_{kT_c}^{(k+1)T_c} n'(t)dt \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} x_{-1,k} \int_{kT_c}^{(k+1)T_c} \sum_{k=0}^{\infty} \xi_k r(t-kT_c)dt \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} x_{-1,k} T_c \xi_k \\
&= \sum_{k=(m-1)\beta}^{m\beta-1} n_k'
\end{aligned}
\tag{D-9}
$$

where $n_k' = x_{-1,k} T_c \xi_k$. The new noise components $\{n_k'\}$ are also Gaussian. Their mean values are

$$
E[n_k'] = x_{-1,k} T_c E[\xi_k] = x_{-1,k} T_c \overline{\xi_k} \tag{D-10}
$$

and their covariances are

$$
\begin{aligned}
E[n_j' n_k'] &= x_{-1,j} x_{-1,k} T_c^2 E[\xi_j \xi_k] \\
&= x_{-1,k}^2 T_c^2 \sigma_{n'}^2 \delta_{jk}
\end{aligned}
\tag{D-11}
$$

where the last equality is due to the independence of ξ_k's. Therefore, if the noise source $n'(t)$ is to generate the same effect as the AWGN source at the coherent CSK receiver,

$$
E[n_k'] = E[n_k] \Rightarrow x_{-1,k} T_c \overline{\xi_k} = 0 \Rightarrow \overline{\xi_k} = 0 \tag{D-12}
$$

and

$$
\begin{aligned}
& E[n_j' n_k'] = E[n_j n_k] \\
& \Rightarrow x_{-1,k}^2 T_c^2 \sigma_{n'}^2 \delta_{jk} = x_{-1,k}^2 \frac{N_0 T_c}{2} \delta_{jk} \\
& \Rightarrow \sigma_{n'}^2 = \frac{N_0}{2T_c}.
\end{aligned}
\tag{D-13}
$$

Since the mean and variance of $\{\xi_k\}$ are independent of the chaotic signals, it can be concluded that in the analyses of a coherent CSK system with AWGN, the original AWGN noise source can be replaced by an equivalent noise $n'(t)$ given by

$$n'(t) = \sum_{k=0}^{\infty} \xi_k r(t - kT_c) \tag{D-14}$$

where the coefficients $\{\xi_k\}$ are independent Gaussian random variables with zero mean

$$\overline{\xi_k} = 0 \tag{D-15}$$

and variance

$$\sigma_{n'}^2 = \frac{N_0}{2T_c}. \tag{D-16}$$

Appendix E

Error Probability

Given a normal random variable X with mean m_x and variance σ_x^2, its probability density function is given by

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-m_x)^2}{2\sigma_x^2}\right] \tag{E-1}$$

The probability that X is less than zero is derived by

$$\begin{aligned}
\text{Prob}(X<0) &= \int_{-\infty}^{0} f_X(x)dx \\
&= \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-m_x)^2}{2\sigma_x^2}\right]dx \\
&= \int_{-\infty}^{-m_x} \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{y^2}{2\sigma_x^2}\right]dy \\
&= \int_{-\infty}^{-m_x/\sigma_x} \frac{1}{\sqrt{2\pi}} \exp(-\frac{z^2}{2})dz \\
&= \int_{m_x/\sigma_x}^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{t^2}{2})dt
\end{aligned} \tag{E-2}$$

where the following changes of variables have been made: $y = x - m_x$, $z = y/\sigma_x$ and $t = -z$.

Therefore, if $z_{+1}(mT_b)$ is normally distributed with mean $\overline{z_{+1}(mT_b)}$ and variance $\mathrm{var}[z_{+1}(mT_b)]$, the probability that a "–1" is detected is

$$\begin{aligned}
&\mathrm{Prob}(z_{+1}(mT_b) < 0 \,|\, \text{"+1" is transmitted}) \\
&= \int_{\overline{z_{+1}(mT_b)}/\sqrt{\mathrm{var}[z_{+1}(mT_b)]}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{t^2}{2}) dt \\
&= Q\left(\frac{\overline{z_{+1}(mT_b)}}{\sqrt{\mathrm{var}(z_{+1}(mT_b))}} \right)
\end{aligned} \tag{E-3}$$

where

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp(\frac{-t^2}{2}) dt . \tag{E-4}$$

Note also that

$$Q(-x) = 1 - Q(x) . \tag{E-5}$$

Appendix F

Statistical Properties of $X_{i,u,v}(f_i,m_i)$

The statistical properties of $X_{i,u,v}(f_i,m_i)$, defined in Chapter 5 as

$$X_{i,u,v}(f_i,m_i) = \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} s_u(t)s_v(t-\frac{iT_b}{2})dt\,, \tag{F-1}$$

are investigated here for different combinations of u, v and i. We assume that the cubic map $x_{i,n+1} = g(x_{i,n}) = 4x_{i,n}^3 - 3x_{i,n}$ (i = 1, 2, .., N) is used to generate the chaotic coefficients for user i. All symbols have their meanings as defined in the thesis.

F.1 $u = v = i$

$$X_{i,i,i}(f_i,m_i) = \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} s_i(t)s_i(t-\frac{iT_b}{2})dt \tag{F-2}$$

In this case, the reference sample of the ith user correlates with the corresponding data sample. Since the data sample is derived from the reference sample, with a possible factor of -1 due to the binary symbol, a high correlation value is expected. The derivation of $X_{i,i,i}(f_i,m_i)$ is shown below.

$$
\begin{aligned}
X_{i,i,i}(f_i,m_i) &= \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} s_i(t)s_i(t-\frac{iT_b}{2})dt \\
&= d_{i,m_i+(f_i-1)i} \int_{[2(f_i-1)i+m_i-1]T_b/2}^{[2(f_i-1)i+m_i]T_b/2} y^2_{i,m_i,f_i}(t)dt \\
&= d_{i,m_i+(f_i-1)i} T_c \sum_{k=0}^{\alpha-1} x^2_{i,k+\alpha[(m_i-1)+(f_i-1)i]} \\
&= d_{i,m_i+(f_i-1)i} T_c \alpha \gamma_{x_i}\{\alpha[(m_i-1)+(f_i-1)i],\alpha[(m_i-1)+(f_i-1)i],\alpha\}
\end{aligned}
\tag{F-3}
$$

It has been shown in Section 2.3.4 that

$$\gamma_{x_i}\{\alpha[(m_i-1)+(f_i-1)i],\alpha[(m_i-1)+(f_i-1)i],\alpha\}$$

follows a normal distribution with mean

$$\overline{\gamma_{x_i}\{\alpha[(m_i-1)+(f_i-1)i],\alpha[(m_i-1)+(f_i-1)i],\alpha\}} = \begin{cases} 0.5 & \alpha = 100 \\ 0.5 & \alpha = 1000 \end{cases} \tag{F-4}$$

and variance

$$\mathrm{var}\{\gamma_{x_i}[\alpha[(m_i-1)+(f_i-1)i],\alpha[(m_i-1)+(f_i-1)i],\alpha]\} = \begin{cases} 1.24\mathrm{x}10^{-3} & \alpha = 100 \\ 1.24\mathrm{x}10^{-4} & \alpha = 1000. \end{cases} \tag{F-5}$$

Therefore, if the $[(f_i-1)i+m_i]$th transmitted symbol of user i is "+1", i.e., $d_{i,m_i+(f_i-1)i} = +1$, $X_{i,i,i,+1}(f_i,m_i)$ will follow a normal distribution with mean

$$
\begin{aligned}
&\overline{X_{i,i,i,+1}(f_i,m_i)} \\
&= T_c\alpha\overline{\gamma_{x_i}\{\alpha[(m_i-1)+(f_i-1)i],\alpha[(m_i-1)+(f_i-1)i],\alpha\}} \\
&= \begin{cases} 0.5T_c\alpha = 0.25T_b & \alpha = 100 \\ 0.5T_c\alpha = 0.25T_b & \alpha = 1000 \end{cases}
\end{aligned}
\tag{F-6}
$$

and variance

$$\begin{aligned}
&\mathrm{var}[X_{i,i,i,+1}(f_i,m_i)] \\
&= T_c^2\alpha^2\ \mathrm{var}\{\gamma_{x_i}[\alpha[(m_i-1)+(f_i-1)i],\alpha[(m_i-1)+(f_i-1)i],\alpha]\} \\
&= \begin{cases} 1.24\mathrm{x}10^{-3}T_c^2\alpha^2 = 0.31\mathrm{x}10^{-3}T_b^2 & \alpha = 100 \\ 1.24\mathrm{x}10^{-4}T_c^2\alpha^2 = 0.31\mathrm{x}10^{-4}T_b^2 & \alpha = 1000. \end{cases}
\end{aligned} \tag{F-7}$$

Similarly, if $d_{i,(f_i-1)i+m_i} = -1$, $X_{i,i,i,-1}(f_i,m_i)$ will be normally distributed with mean

$$\overline{X_{i,i,i,-1}(f_i,m_i)} = \begin{cases} -0.25T_b & \alpha = 100 \\ -0.25T_b & \alpha = 1000 \end{cases} \tag{F-8}$$

and variance

$$\mathrm{var}[X_{i,i,i,-1}(f_i,m_i)] = \begin{cases} 0.31\mathrm{x}10^{-3}T_b^2 & \alpha = 100 \\ 0.31\mathrm{x}10^{-4}T_b^2 & \alpha = 1000. \end{cases} \tag{F-9}$$

F.2 $u = v, u \neq i$

$$X_{i,u,u}(f_i,m_i) = \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} s_u(t)s_u(t-\frac{iT_b}{2})dt \tag{F-10}$$

In this case, one reference/data sample of the uth user correlates with another reference/data sample i half-bit slots away. For the uth user, the reference sample and its corresponding data sample are separated by u half-bit slots. Therefore, if $u \neq i$, low correlation is expected between the reference/data samples separated by i half-bit slots. Denote the two reference/data samples by $Y_{u1}(t)$ and $Y_{u2}(t)$ respectively, where $Y_{u1}(t) = Z_{u1}(t)A_{u1}$ and $Y_{u2}(t) = Z_{u2}(t)A_{u2}$. For q = 1, 2, A_{uq} is defined as

$$A_{uq} = \begin{cases} +1 & \begin{array}{l} Y_{uq}(t) \text{ is the reference sample} \\ \text{or } Y_{uq}(t) \text{ is the data sample transmitting the symbol "+1"} \end{array} \\ -1 & Y_{uq}(t) \text{ is the data sample transmitting the symbol "−1"} \end{cases} \tag{F-11}$$

while $Z_{uq}(t)$, denoted by

$$Z_{uq}(t) = \sum_{k=0}^{\alpha-1} x_{u,uq+k} r[t - (kT_c + (m_i - 1)\frac{T_b}{2} + (f_i - \frac{1}{2})iT_b)], \tag{F-12}$$

represents the reference sample produced by the chaotic generator of user u with $u1 \neq u2$.

The integral $X_{i,u,u}(f_i, m_i)$ is now re-written as

$$\begin{aligned} & X_{i,u,u}(f_i, m_i) \\ &= \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} Y_{u1}(t) Y_{u2}(t) dt \\ &= A_{u1} A_{u2} \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} Z_{u1}(t) Z_{u2}(t) dt \\ &= A_{uu} \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} \sum_{k=0}^{\alpha-1} x_{u,u1+k} x_{u,u2+k} r[t - (kT_c + (m_i - 1)\frac{T_b}{2} + (f_i - \frac{1}{2})iT_b)] dt \\ &= A_{uu} T_c \sum_{k=0}^{\alpha-1} x_{u,u1+k} x_{u,u2+k} \\ &= A_{uu} T_c \alpha \gamma_{x_u}(u1+k, u2+k, \alpha) \end{aligned} \tag{F-13}$$

where $A_{uu} = A_{u1} A_{u2}$.

First, A_{uu} and $\gamma_{x_u}(u1+k, u2+k, \alpha)$ are independent random variables. Second, since A_{u1} and A_{u2} are independent random variables with values ± 1, their product A_{uu}

can only take the same values ±1. It has been shown in Section 2.3.4 that for $\alpha = 100$ and 1000, $\gamma_{x_u}(u1+k, u2+k, \alpha)$ follows a normal distribution with zero mean, i.e.,

$$\overline{\gamma_{x_u}(u1+k, u2+k, \alpha)} = 0, \tag{F-14}$$

and variance

$$\mathrm{var}[\gamma_{x_u}(u1+k, u2+k, \alpha)] = \begin{cases} 2.50\mathrm{x}10^{-3} & \alpha = 100 \\ 2.50\mathrm{x}10^{-4} & \alpha = 1000. \end{cases} \tag{F-15}$$

For brevity, we let W_{uu} denote $\alpha T_c \gamma_{x_u}(u1+k, u2+k, \alpha)$. Therefore, W_{uu} is normally distributed with mean

$$\overline{W_{uu}} = 0 \tag{F-16}$$

and variance

$$\mathrm{var}(W_{uu}) = \begin{cases} 2.50\mathrm{x}10^{-3}\alpha^2 T_c^2 = 0.625\mathrm{x}10^{-3} T_b^2 & \alpha = 100 \\ 2.50\mathrm{x}10^{-4}\alpha^2 T_c^2 = 0.625\mathrm{x}10^{-4} T_b^2 & \alpha = 1000. \end{cases} \tag{F-17}$$

To find the distribution of $X_{i,u,u}(f_i, m_i)$, we first evaluate the probability that $w \le X_{i,u,u}(f_i, m_i) \le w + \Delta w$, where Δw is a very small interval.

$$
\begin{aligned}
&P(w \le X_{i,u,u}(f_i, m_i) \le w + \Delta w) \\
&= P(w \le W_{uu} \le w + \Delta w) P(A_{uu} = +1) + P(-w \ge W_{uu} \ge -w - \Delta w) P(A_{uu} = -1) \\
&= \left[\frac{1}{\sqrt{2\pi \operatorname{var}(W_{uu})}} \exp\left(\frac{-(w - \overline{W_{uu}})^2}{2 \operatorname{var}(W_{uu})} \right) \Delta w \right] P(A_{uu} = +1) \\
&\quad + \left[\frac{1}{\sqrt{2\pi \operatorname{var}(W_{uu})}} \exp\left(\frac{-(-w - \overline{W_{uu}})^2}{2 \operatorname{var}(W_{uu})} \right) \Delta w \right] P(A_{uu} = -1) \\
&= \left[\frac{1}{\sqrt{2\pi \operatorname{var}(W_{uu})}} \exp\left(\frac{-w^2}{2 \operatorname{var}(W_{uu})} \right) \Delta w \right] [P(A_{uu} = +1) + P(A_{uu} = -1)] \\
&= \frac{1}{\sqrt{2\pi \operatorname{var}(W_{uu})}} \exp\left(\frac{-w^2}{2 \operatorname{var}(W_{uu})} \right) \Delta w
\end{aligned}
\tag{F-18}
$$

where $P(A_{uu} = +1)$ and $P(A_{uu} = -1)$ represent the probabilities that A_{uu} equals +1 and –1 respectively. Hence, the probability density function of $X_{i,u,u}(f_i, m_i)$ is identical to that of W_{uu}. Therefore, $X_{i,u,u}(f_i, m_i)$ also follows a normal distribution with mean

$$\overline{X_{i,u,u}(f_i, m_i)} = \overline{W_{uu}} = 0 \tag{F-19}$$

and variance

$$\operatorname{var}[X_{i,u,u}(f_i, m_i)] = \operatorname{var}(W_{uu}) = \begin{cases} 0.625\text{x}10^{-3} T_b^2 & \alpha = 100 \\ 0.625\text{x}10^{-4} T_b^2 & \alpha = 1000. \end{cases} \tag{F-20}$$

F.3 $u \neq v$

$$X_{i,u,v}(f_i, m_i) = \int_{[2(f_i - 1)i + i + m_i - 1]T_b/2}^{[2(f_i - 1)i + i + m_i]T_b/2} s_u(t) s_v(t - \frac{iT_b}{2}) dt \tag{F-21}$$

In this case, one reference/data sample of the uth user correlates with the reference/data sample of another user (vth user) i half-bit slots away. Since the samples

are generated by chaos generators with different initial conditions, low correlation is expected. Denote the two reference/data samples by $Y_u(t)$ and $Y_v(t)$ respectively, where $Y_u(t) = Z_u(t)A_u$ and $Y_v(t) = Z_v(t)A_v$. Similar to the previous case, $Z_u(t)$ and $Z_v(t)$ represent the reference samples generated by the chaos generators. They are denoted by

$$Z_u(t) = \sum_{k=0}^{\alpha-1} x_{u,u'+k}\, r[t - (kT_c + (m_i - 1)\frac{T_b}{2} + (f_i - \frac{1}{2})iT_b)] \tag{F-22}$$

and

$$Z_v(t) = \sum_{k=0}^{\alpha-1} x_{v,v'+k}\, r[t - (kT_c + (m_i - 1)\frac{T_b}{2} + (f_i - \frac{1}{2})iT_b)] \ . \tag{F-23}$$

Moreover,

$$A_u[A_v] = \begin{cases} +1 & \begin{array}{l} Y_u(t)[Y_v(t)] \text{ is the reference sample} \\ \text{or } Y_u(t)[Y_v(t)] \text{ is the data sample transmitting the symbol "+1"} \end{array} \\ -1 & Y_u(t)[Y_v(t)] \text{ is the data sample transmitting the symbol "−1"} \end{cases} \tag{F-24}$$

$X_{i,u,v}(f_i, m_i)$ is now given by

$$\begin{aligned} & X_{i,u,v}(f_i, m_i) \\ &= \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} Y_u(t)Y_v(t)dt \\ &= A_u A_v \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} Z_u(t)Z_v(t)dt \\ &= A_{uv} \int_{[2(f_i-1)i+i+m_i-1]T_b/2}^{[2(f_i-1)i+i+m_i]T_b/2} \sum_{k=0}^{\alpha-1} x_{u,u'+k}\, x_{v,v'+k}\, r[t - (kT_c + (m_i - 1)\frac{T_b}{2} + (f_i - \frac{1}{2})iT_b)]dt \\ &= A_{uv}T_c \sum_{k=0}^{\alpha-1} x_{u,u'+k}\, x_{v,v'+k} \\ &= A_{uv}T_c\alpha\gamma_{x_{uv}}(u'+k, v'+k, \alpha). \end{aligned}$$

(F-25)

where $A_{uv} = A_u A_v$.

Using the results in Section 2.3.4 again, $\gamma_{x_{uv}}(u'+k, v'+k, \alpha)$ can be shown to follow a normal distribution for $\alpha =$ 100 and 1000. By repeating the procedures in the previous section, it can be proved easily that $X_{i,u,v}(f_i, m_i)$ is also normally distributed with mean

$$\overline{X_{i,u,v}(f_i, m_i)} = 0 \tag{F-26}$$

and variance

$$\mathrm{var}[X_{i,u,v}(f_i, m_i)] = \begin{cases} 0.625\mathrm{x}10^{-3} T_b^2 & \alpha = 100 \\ 0.625\mathrm{x}10^{-4} T_b^2 & \alpha = 1000. \end{cases} \tag{F-27}$$

REFERENCES

[Alli 96] K.T. Alligood, T.D. Sauer and J.A. Yorke, *Chaos: An Introduction to Dynamical Systems*, New York: Springer-Verlag, 1996.

[Blue 00] Bluetooth website, http://www.bluetooth.com, 2000.

[Carr 91] T.L. Carroll and L.M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. on Circuits and Systems*, Vol. 38, No. 4, April 1991, pp. 453-456.

[Carr 99] T.L. Carroll and L.M. Pecora, "Using multiple attractor chaotic systems for communication," *Chaos*, No. 9, 1999, pp. 445-451.

[Clar 96] Bill Clarke, *GPS Aviation Applications*, McGraw Hill, 1996.

[Deva 92] R.L. Devaney, *A First Course in Chaotic Dynamical Systems*, New York: Addison-Wesley, 1992.

[Dixo 94] R.C. Dixon, *Spread Spectrum Systems with Commercial Applications*, 3rd ed., John Wiley & Sons, 1994.

[Glob 86] Global Positioning Systems, Papers published in *Navigation*, Vols. I-III, Washington, D.C.: Institute of Navigation, 1986.

[Heid 94] G. Heidari-Bateni and C.D. McGillem, "A chaotic direct-sequence spread spectrum communication system," *IEEE Trans. on Communications*, Vol. 42, No.2-4, Feb.-Apr. 1994, pp.1524-1527.

[Ieee 99] *IEEE Standard 802.11*, USA, 1999.

[Itoh 95] M. Itoh and H. Murakami, "New communication systems via chaotic synchronizations and modulation," *IEICE Trans. Fundamentals*, E78-A(3), 1995, pp. 285-290.

[Jako 98] Z. Jako, "Performance improvement of DCSK modulation," *Proceedings, 6th International Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 98)*, Budapest, Hungary, July 1998, pp.119-122.

[Kenn 98a] M.P. Kennedy, G. Kolumban, G. Kis and Z. Jako, "Recent advances in communicating with chaos," *Proceedings, International Symposium on Circuits and Systems, ISCAS '98*, May 1998, Montery, California, USA, pp. 461 - 464.

[Kenn 98b] M.P. Kennedy, "Chaotic communications: from chaotic synchronization to FM-DCSK," *Proceedings, 6th International Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 98)*, Budapest, Hungary, July 1998, pp.31-40.

[Kenn 98c] G. Kolumban, M.P. Kennedy and L.O. Chua, "The role of synchronization in digital communications using chaos - Part II: Chaotic modulation and chaotic synchronization," *IEEE Trans. on Circuits and Systems I*, Vol. 45, No. 11, Nov. 1998, pp.1129 -1140.

[Kenn 99] M.P. Kennedy and G. Kolumban, "Digital communications using chaos," in G. Chen, *Controlling Chaos and Bifurcations in Engineering Systems*, pp. 477-500, New York: CRC Press, 1999.

[Kis 98a] G. Kis, Z. Jako, M.P. Kennedy and G. Kolumban, "Chaotic communications without synchronization," *Proceedings, 6th IEE Conference on Telecommunications*, Edinburgh, UK, March 1998, pp.49-53.

[Kis 98b] G. Kis, "Required bandwidth of chaotic signals used in chaotic modulation schemes," *Proceedings, 6th International Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 98)*, Budapest, Hungary, July 1998, pp.113-117.

[Koca 92] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation and Chaos*, Vol. 2, No. 3, March 1992, pp. 709-713.

[Kolu 97a] G. Kolumban, M.P. Kennedy and G. Kis, "Multilevel differential chaos keying," *Proceedings, 5th International Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 97)*, Moscow, Russia, June 1997, pp. 191-196.

[Kolu 97b] G. Kolumban, G. Kis, M.P. Kennedy and Z. Jako, "FM-DCSK: a new and robust solution to chaos communications," *Proceedings, NOLTA'97*, Hawaii, November 1997, pp. 117-120.

[Kolu 98] G. Kolumban, "Performance evaluation of chaotic communications systems: Determination of low-pass equivalent model," *Proceedings, 6th International Specialist Workshop on Nonlinear Dynamics of Electronics Systems (NDES 98)*, Budapest, Hungary, July 1998, pp.41-51.

[Mazz 97] G. Mazzini, G. Setti and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA. Part I: system modeling and results," *IEEE Trans. on Circuits and Systems – I*, Vol. 44, No. 10, October 1997, pp. 937-947.

[Mazz 98] G. Mazzini, G. Setti and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA. Part II: some theoretical performance bounds," *IEEE Trans. on Circuits and Systems – I*, Vol. 45, No. 10, April 1998, pp. 496-506.

[Mull 93] T. Mullin, *The Nature of Chaos*, New York: Oxford University Press, 1993.

[Pete 95] R.L. Peterson, R.E. Ziemer and, D.F. Borth, *Introduction to Spread Spectrum Communications*, Singapore: Prentice Hall, 1995.

[Proa 94] J.G. Proakis and M. Salehi, *Communications Systems Engineering*, Englewood Cliffs, Prentice Hall, 1994.

[Proa 95] J.G. Proakis, *Digital Communications*, third edition, McGraw Hill, 1995.

[Ross 93] S.M. Ross, *Introduction to Probability Models*, 5th Edition, New York: Academic Press, 1993.

[Sett 99] G. Setti, R. Rovatti and G. Mazzini, "Synchronization mechanism and optimization of spreading sequences in chaos-based DS-CDMA systems," *IEICE Trans. on Fundamentals*, Vol. E82-A, No. 9, September 1999, pp.1737-1746.

[TIA 95] *TIA/EIA Interim Standard IS-95-A Standard*, USA, May 1995.

[Vite 95] A.J. Viterbi, *CDMA-Principles of Spread Spectrum Communication*, Addison-Wesley, 1995.

[Yang 97] T. Yang and L.O. Chua, "Chaotic digital code-division multiple access (CDMA) communication systems," *Int. J. Bifurcation and Chaos*, Vol. 7, No. 12, Dec. 1997, pp. 2789-805.