

PERFORMANCE EVALUATION OF DS-CDMA SYSTEM USING CHAOTIC BINARY SEQUENCES

Mahalinga V. Mandi¹, K. N. Hari Bhat² and R. Murali³

¹ Associate Professor, Department of Electronics & Communication Engineering, Dr. Ambedkar Institute of Technology, INDIA.

² Dean Academic, Professor & Head, Department of Electronics & Communication Engineering, Nagarjuna College of Engineering & Technology, INDIA.

³ Professor, Department of Mathematics, Dr. Ambedkar Institute of Technology, INDIA.

ABSTRACT

In this paper generation of binary sequences derived from chaotic sequences defined over Z_4 is proposed. The six chaotic map equations considered in this paper are Logistic map, Tent Map, Cubic Map, Quadratic Map and Bernoulli Map. Using these chaotic map equations, sequences over Z_4 are generated which are converted to binary sequences using polynomial mapping. Segments of sequences of different lengths are tested for cross correlation and linear complexity properties. It is found that some segments of different length of these sequences have good cross correlation and linear complexity properties. The Bit Error Rate performance in DS-CDMA communication systems using these binary sequences is found to be better than Gold sequences and Kasami sequences.

KEYWORDS

DS-CDMA, Chaos, Chaotic map, Polynomial mapping

1. INTRODUCTION

A chaotic map $x_{n+1} = F(x_n)$ is typically a non-linear discrete dynamical iteration equation, which exhibits some sort of chaotic behavior. Chaos is characterized by deterministic, nonlinear, non-periodic, non-converging and bounded behavior. The main characteristic of chaos is the sensitive dependence on initial conditions. Certain maps exhibit this property and it is possible to achieve chaotic behaviour by recursively evaluating these maps in discrete time. The sequences generated by iterating a given chaotic map will diverge to different trajectories in a few cycles even though their initial conditions differ by less than 1% [1].

One of the well known one-dimensional iterative maps which exhibit chaotic properties is the Logistic Map [2]. The other chaotic maps which are of interest are Tent map [3], Cubic map [4], Quadratic map [5] and Bernoulli map [4]. Chaotic sequences are easy to generate and store. Only few parameters and functions are needed for generating very long sequences. In addition, an enormous number of different sequences can be generated simply by changing its initial condition. The inherent properties of chaotic sequences make them suitable for communication systems. It also enhances the security of transmission.

The applications of chaotic sequences generated by nonlinear dynamical systems to direct sequence spread-spectrum (DS/SS) systems is discussed in [6] - [12]. As there are an infinite number of sequences that can be generated by any chaotic system, exploiting such systems for

generating spreading sequences for use in DS/SS systems have received a lot of attention in recent times. In recent years several methods to generate chaotic binary sequences using Threshold function [13] and Coupled Chaotic Systems [14] are proposed in the literature.

Generation of discrete sequences over Z_4 from chaotic sequences is discussed in [15]. Using binary conversion, binary sequences are obtained from chaotic sequences over Z_4 . Their correlation and linear complexity properties are discussed in [16] and [17]. Deriving binary sequences from sequence over Z_4 using polynomial mapping is discussed in [18]. The three polynomial mappings considered in [18] for $x \in Z_4$ is given by,

$$P_1(x) = (x^2 - x) \text{ mod } 4 \quad (1)$$

$$P_3(x) = (x^2 + x) \text{ mod } 4 \quad (2)$$

$$P_2(x) = 2x \text{ mod } 4 \text{ and} \quad (3)$$

In this paper chaotic binary sequences are obtained from sequence over Z_4 using polynomial mappings given by equation (1). The generated binary sequences are investigated for pairwise cross correlation and linear complexity properties. The six chaotic map equations such as Logistic map, Tent Map, Cubic Map, Quadratic Map and Bernoulli Map are considered for generating sequences over Z_4 .

The work is organized as follows: In Section 2, a brief introduction to chaotic functions is presented. In Section 3, we present generation of chaotic binary sequences, applying polynomial mapping [18] to sequence over Z_4 . In Section 4, Cross Correlation and linear complexity properties of generated binary sequences and their application in DS-CDMA are investigated. Finally, Section 5 contains concluding remarks.

2. INTRODUCTION TO CHAOTIC FUNCTIONS

The different chaotic map equations considered in this work are as follows,

1) Logistic Map equations [2]

$$\text{Logistic Map (1): } X_{k+1} = rX_k(1 - X_k), \text{ defined over real, } 0 < x < 1 \quad (4)$$

where r is called bifurcation parameter or control parameter and $3.57 < r < 4$.

$$\text{Logistic Map (2): } X_{k+1} = (1 - rX_k^2) \quad -1 < x < 1 \quad (5)$$

where $1.72 < r < 2$.

2) Tent Map equation [3]

$$X_{k+1} = \begin{cases} X_k/0.7 & \text{for } X_k \leq 0.7 \\ (1 - X_k)/0.3 & \text{otherwise} \end{cases} \quad 0 < x < 1 \quad (6)$$

3) Cubic Map equation [4]

$$X_{k+1} = (4X_k^3 - 3X_k) \quad -1 < x < 1 \quad (7)$$

4) Quadratic Map equation [5]

$$X_{k+1} = (r - 4X_k^2) \quad -0.5 < x < 0.5 \quad (8)$$

Control parameter r is chosen to be $0.36 < r < 0.5$

5) Bernoulli Map equation [4]

$$X_{k+1} = \begin{cases} rX_k + 0.5 & \text{for } X_k < 0 \\ rX_k - 0.5 & \text{for } X_k \geq 0 \end{cases} \quad -0.5 < x < 0.5 \quad (9)$$

Control parameter r is chosen to be $1.2 < r < 2$

For the choice of control parameter r, within the range given along with the equation (4), (5), (8) and (9), the sequence produced is non-periodic and non-converging. Even with two initial values differing by a very small value, the resulting sequences are highly uncorrelated.

3. GENERATION OF BINARY SEQUENCES DERIVED FROM CHAOTIC SEQUENCE OVER Z_4 USING POLYNOMIAL MAPPING

A scheme of generating chaotic sequence over Z_4 is shown in figure 1. In this case each element Y_k of sequence $\{x_i\}$ is multiplied by a large integer n and the fraction part is discarded. The integer part is Q_k . The large value of integer part Q_k is then reduced to small integer Y_k modulo 4. It is necessary that $n > 4$. Thus the sequence $\{Y_k\}$ is over Z_4 . A method of deriving binary sequence from sequence over Z_4 using polynomial mapping $P_1(x) = (x^2 - x) \text{ mod } 4$ is considered in this paper. Any integer Y_k in the range 0 to 3 in the sequence $\{Y_k\}$ is mapped to $\{0, 2\}$. The sequence over $\{0, 2\}$ is further mapped to binary sequence by mapping $(0, 2) \in Z_4$ to $(1, -1)$ in binary. Mapping from Z_4 to binary is shown in Table 1.

Table 1. Binary mapping using $P_1(x) = (x^2 - x) \text{ mod } 4$

x	0	1	2	3
$P_1(x) = (x^2 - x) \text{ mod } 4$	0	0	2	2
Binary mapping	1	1	-1	-1

Thus model shown in Figure 1 can be used to derive discrete sequence $\{Y_k\}$ over Z_4 ; where $Y_k \in \{0, 1, 2, 3\}$ or binary $\{b_k\}$, from the chaotic sequence $\{X_k\}$.

The scheme is governed by equation (10) and is given by

$$Y_k = \lfloor \lfloor \{X_k\} n \rfloor \rfloor \text{ mod } 4, \quad (10)$$

where $\lfloor \{X_k\} n \rfloor = Q_k$, integer part of product $X_k n$.

Using polynomial mapping, the length of the resulting binary sequence turns out to be same as sequence over Z_4 .

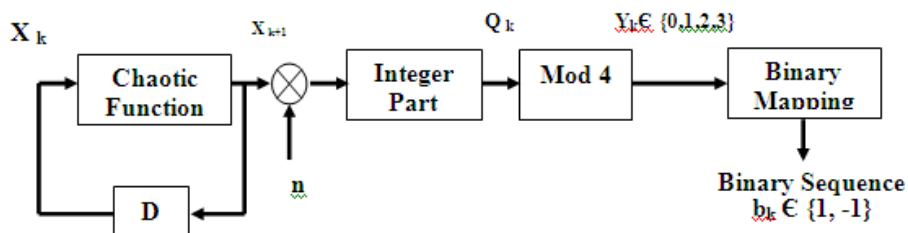


Figure 1. Scheme of generating chaotic binary sequence

4. CROSS CORRELATION (CCR) AND LINEAR COMPLEXITY (LC) PROPERTIES

4.1. Cross Correlation Property

Definition: The normalized cyclic Hamming cross correlation function of two sequences x and y of length N symbols is defined [19] as

$$R_{xy}(\tau) = \frac{n_\tau - d_\tau}{N} \quad \text{Where } 0 \leq \tau \leq N-1. \quad (11)$$

Where n_τ and d_τ are the number of locations at which symbols agree and disagree respectively between the two sequences x and y . τ is the number of locations by which one sequence say y is shifted with respect to the other sequence x . It is easy to see that when symbols of the sequence are 1 and -1, the normalized cyclic cross correlation values and normalized cyclic Hamming cross correlation values are same.

4.2. Linear Complexity

Definition: Linear complexity [20] of a binary sequence of finite length is the length of the shortest LFSR that generates the same sequence. Berlekamp – Massey algorithm is an efficient algorithm for determining the linear complexity of binary sequence of finite length. The binary sequence with values 1, -1 is changed to 1, 0 to apply Berlekamp – Massey algorithm.

4.3. Properties of Segments of Chaotic Binary Sequences

For each of the six chaotic functions discussed in Section 2, real valued sequence $\{x_k\}$ is generated by choosing arbitrarily the initial values x_0 and appropriate bifurcation parameter r as given in equations (4) to (9). This real valued sequence $\{x_k\}$ is converted to sequence over Z_4 using the model shown in Fig 1 by arbitrarily choosing value of multiplication factor ‘ n ’ reducing the integer part to modulo 4. The sequence over Z_4 is converted to binary using polynomial mapping given by equation (1). The resulting binary sequence is an infinite sequence. To study the properties of the sequence, as an example, first 12600 bits of the generated binary sequence as shown in Fig 2 are considered which is divided into 63 bit non-overlapping segments. The number of segments of 63 bit that we get is 200. Each of these segments is numbered as Segment 1, Segment 2, ... and is shown in equation (12).

$$\text{Binary Sequence} = \underbrace{b_0, b_1, \dots, b_{62}}_{\text{Segment 1}}, \underbrace{b_{63}, b_{64}, \dots, b_{125}}_{\text{Segment 2}}, \dots, \underbrace{b_{12536}, \dots, b_{12599}}_{\text{Segment 200}} \quad (12)$$

Similarly non-overlapping segments of 127 bits and 255 bits are considered. The linear complexity of non-overlapping segments of sequences of different lengths (63, 127 and 255 bits) is computed using Berlekamp – Massey algorithm and pairwise cross correlation values are computed using equation (11). The number of sequences having pairwise cross correlation values denoted by α is determined for different α values based on the segment lengths. The arbitrarily chosen values of multiplication factor n are from $\{5, 6, 7 \dots 10\}$. We consider Polynomial mapping given by equation (1) for all the six chaotic map equations considered.

If we consider Gold sequence of length 63 their pairwise CCR value α is less than or equal to 0.2698 [21] and there are 65 Gold sequences with linear complexity 12. For Gold sequences of length 127 the pairwise CCR value α is less than or equal to 0.1339 and there are 129 Gold

sequences with linear complexity 14. If the Gold sequence is of length 255 bits then their pairwise CCR value α is less than or equal to 0.1294 and there are 257 Gold sequences with linear complexity 16. In the proposed scheme it is possible to obtain also sequences of same length whose pairwise CCR value α is less than that of Gold sequences and linear complexity greater than that of Gold sequences.

4.4. Deriving binary sequence using Polynomial mapping given by equation (1)

4.4.1. Logistic map equation

First we consider Logistic map equation given by equation (4) where initial value x_0 is taken as 0.4 and bifurcation parameter $r = 3.99$, the number of sequences having pairwise CCR value less than α are tabulated in Table 2. First column of Table 2 gives trial number with different n . Second column give the value of n chosen. The number of sequences of different lengths having pairwise CCR value less than or equal to α is given in the remaining columns.

Details of trial number 1 are given in first row of Table 2. For n value chosen as 5, there are 25 segments of sequences whose pairwise $\alpha \leq 0.2063$, 46 sequences whose pairwise $\alpha \leq 0.2381$ and 73 sequences whose pairwise $\alpha \leq 0.2698$ of length 63 bits. Likewise the details are tabulated for Trial numbers 2 to 6 for different arbitrarily chosen values of n .

Table 2. Number of sequences having pairwise CCR value less than or equal to α with initial value $x_0 = 0.4$ and $r = 3.99$

Trial Number	n value chosen	Number of sequences having pairwise CCR value less than α								
		For segments of length 63 bits			For segments of length 127 bits			For segments of length 255 bits		
		$\alpha \leq 0.2063$	$\alpha \leq 0.2381$	$\alpha \leq 0.2698$	$\alpha \leq 0.1023$	$\alpha \leq 0.1181$	$\alpha \leq 0.1339$	$\alpha \leq 0.1137$	$\alpha \leq 0.1216$	$\alpha \leq 0.1294$
1	5	25	46	73	45	75	138	67	125	275
2	6	23	47	71	49	76	130	62	134	278
3	7	26	46	69	52	76	135	75	127	301
4	8	27	45	73	50	72	136	70	133	310
5	9	22	44	74	44	76	127	76	141	299
6	10	25	46	70	41	75	125	69	123	267

The linear complexity is determined using Berlekamp – Massey algorithm and is shown in Table 3.

Table 3. Linear complexity of Gold sequences and proposed sequences using Logistic map equation (1)

Length of sequence	Linear complexity in case of Gold sequences	Linear complexity of proposed scheme
63	12	29 to 35
127	14	58 to 65
255	16	125 to 131

Next we consider logistic map given by equation (5) with the same initial value $x_0 = 0.4$ and bifurcation parameter $r = 1.99$. The number of sequences having pairwise CCR value less than or equal to α is tabulated in Table 3.

Details of trial number 1 are given in first row of Table 4. For $n = 5$ there are 23 sequences whose pairwise $\alpha \leq 0.2063$, 40 sequences whose pairwise $\alpha \leq 0.2381$ and 72 sequences of length 63 bits whose pairwise $\alpha \leq 0.2698$. Likewise the details are tabulated for Trial numbers 2 to 6 for different arbitrarily chosen values of n .

Table 4. Number of sequences having pairwise CCR value less than or equal to α with initial value $x_0 = 0.4$ and $r = 1.99$

Trial Number	n value chosen	Number of sequences having pairwise CCR value less than α								
		For segments of length 63 bits			For segments of length 127 bits			For segments of length 255 bits		
		$\alpha \leq 0.2063$	$\alpha \leq 0.2381$	$\alpha \leq 0.2698$	$\alpha \leq 0.1023$	$\alpha \leq 0.1181$	$\alpha \leq 0.1339$	$\alpha \leq 0.1137$	$\alpha \leq 0.1216$	$\alpha \leq 0.1294$
1	5	23	40	72	48	75	136	70	119	269
2	6	26	47	72	50	70	146	61	125	288
3	7	21	41	71	44	68	135	68	127	298
4	8	28	43	70	46	78	134	69	135	295
5	9	29	42	73	47	76	129	71	131	301
6	10	23	41	72	43	69	130	65	125	275

4.4.2. Tent map equation

Tent map equation given by equation (6) is considered with initial value $x_0 = 0.4$. As in the earlier cases the results for pairwise CCR value less than or equal to α are summarized in Table 5.

Table 5. Number of sequences having pairwise CCR value less than or equal to α with initial value $x_0 = 0.4$

Trial Number	n value chosen	Number of sequences having pairwise CCR value less than α								
		For segments of length 63 bits			For segments of length 127 bits			For segments of length 255 bits		
		$\alpha \leq 0.2063$	$\alpha \leq 0.2381$	$\alpha \leq 0.2698$	$\alpha \leq 0.1023$	$\alpha \leq 0.1181$	$\alpha \leq 0.1339$	$\alpha \leq 0.1137$	$\alpha \leq 0.1216$	$\alpha \leq 0.1294$
1	5	27	45	70	50	71	135	67	115	279
2	6	21	40	73	51	69	129	66	117	290
3	7	28	40	68	46	68	141	64	110	301
4	8	26	43	69	42	65	138	62	109	275
5	9	26	42	71	49	70	136	70	125	286
6	10	27	39	65	41	72	130	67	123	265

4.4.3. Cubic map equation

Cubic map equation given by equation (7) is considered next with initial value $x_0 = 0.4$. As in the earlier cases the results for pairwise CCR value less than or equal to α are summarized in Table 6 for $n = 5, 6, 7 \dots 10$.

Table 6. Number of sequences having pairwise CCR value less than or equal to α with initial value $x_0 = 0.4$

Trial Number	n value chosen	Number of sequences having pairwise CCR value less than α								
		For segments of length 63 bits			For segments of length 127 bits			For segments of length 255 bits		
		$\alpha \leq 0.2063$	$\alpha \leq 0.2381$	$\alpha \leq 0.2698$	$\alpha \leq 0.1023$	$\alpha \leq 0.1181$	$\alpha \leq 0.1339$	$\alpha \leq 0.1137$	$\alpha \leq 0.1216$	$\alpha \leq 0.1294$
1	5	29	40	73	53	66	130	69	114	290
2	6	23	45	70	45	72	127	62	112	275
3	7	23	45	74	47	66	136	69	99	267
4	8	27	42	75	42	68	135	59	117	276
5	9	23	40	72	51	70	130	66	109	295
6	10	22	41	71	48	67	135	68	105	291

In this case also there are sequences whose pairwise CCR value is less than that of Gold sequences and the number of sequences is more than Gold sequences.

4.4.4. Quadratic map equation

Quadratic map equation given by equation (8) is considered next with initial value $x_0 = 0.4$, bifurcation parameter $r = 0.4$. The results for pairwise CCR value less than or equal to α are summarized in Table 7.

Table 7. Number of sequences having pairwise CCR value less than or equal to α with initial value $x_0 = 0.4$ and $r = 0.4$

Trial Number	n value chosen	Number of sequences having pairwise CCR value less than α								
		For segments of length 63 bits			For segments of length 127 bits			For segments of length 255 bits		
		$\alpha \leq 0.2063$	$\alpha \leq 0.2381$	$\alpha \leq 0.2698$	$\alpha \leq 0.1023$	$\alpha \leq 0.1181$	$\alpha \leq 0.1339$	$\alpha \leq 0.1137$	$\alpha \leq 0.1216$	$\alpha \leq 0.1294$
1	5	29	38	62	53	60	135	57	112	267
2	6	23	46	67	45	70	138	73	108	295
3	7	23	42	72	47	70	127	67	103	290
4	8	27	44	69	42	73	145	68	109	291
5	9	23	40	70	51	65	156	71	115	256
6	10	22	39	71	48	67	144	66	117	265

4.4.5. Bernoulli map equation

Bernoulli map equation given by equation (9) is considered with initial value $x_0 = 0.4$, bifurcation parameter $r = 1.99$ and the results for pair wise CCR value less than or equal to α are summarized in Table 8.

The properties of segments of binary sequences of different lengths derived from sequence over Z_4 using different chaotic map equations are almost same. It is also seen that the properties of binary sequences derived from sequences over Z_4 using polynomial mapping given by equations (2) and (3) are almost identical.

Table 8. Number of sequences having pair wise CCR value less than or equal to α with initial value $x_0 = 0.4$ and $r = 1.99$

Trial Number	n value chosen	Number of sequences having pair wise CCR value less than α								
		For segments of length 63 bits			For segments of length 127 bits			For segments of length 255 bits		
		$\alpha \leq 0.2063$	$\alpha \leq 0.2381$	$\alpha \leq 0.2698$	$\alpha \leq 0.1023$	$\alpha \leq 0.1181$	$\alpha \leq 0.1339$	$\alpha \leq 0.1137$	$\alpha \leq 0.1216$	$\alpha \leq 0.1294$
1	5	25	39	72	43	56	128	65	115	267
2	6	27	43	64	45	61	145	64	119	285
3	7	21	40	68	47	60	136	63	109	292
4	8	25	36	67	42	67	129	69	115	290
5	9	24	45	70	51	69	142	71	113	265
6	10	26	42	71	48	71	140	68	108	269

The linear complexities of proposed sequences are more or less the same for sequences generated using different chaotic functions.

4.5. Bit Error Rate (BER) Performance

In a DS-CDMA system the average BER performance depends mainly on the correlation properties of the spreading sequences assigned to the users. In order to have low interference between users it is necessary to select sets of sequences that form a quasi-orthogonal set. This assumes desirable cross-correlation properties. Most DS-CDMA systems presented have used binary PN sequences including Gold sequences and Kasami sequences that possess some quasi-orthogonality correlation properties.

A new family of spreading sequences is represented by chaotic sequences, generated from the orbits of some dynamical discrete systems. These sequences represent noise-like features that make them good for DS-CDMA systems. The pseudo-chaotic systems generate long periodic sequences and their time evolution (their orbit) depends totally on the initial state of the system. So, a single system, described by its discrete chaotic map, can generate a very large number of distinct pseudo-chaotic sequences, each sequence being uniquely specified by its initial value. This dependency on the initial state and the nonlinear character of the discrete map make the DS-CDMA system using these sequences more secure.

A simplified diagram of a K-user CDMA system is presented in Fig 2 [19]. In the receiving part (the base station for the uplink direction or a mobile station for the downlink direction) the received signal $S_j(t)$, originating from user j, is given by the expression

$$S_j(t) = \sqrt{2} P_j m_j(t) a_j(t) \cos(\omega_0 t + \theta_j) \quad (13)$$

where P_j is the received power of user j, $a_j(t)$ is the spreading sequence, with the chip period $T_c=T/N$, and $m_j(t)$ is the data sequence for user j, both of them being binary sequences with values ± 1 . The signal $r(t)$ at the input of a receiver is

$$r(t) = \sum_{j=1}^K S_j(t) + n(t) \quad (14)$$

Where $n(t)$ is Additive White Gaussian Noise (AWGN) with two-sided power spectral density (PSD) $N_0/2$. It is considered that different user signals are in synchronism. The correlator output $Z_i^{(j)}$ for user j at the end i^{th} bit period T is given by,

$$Z_i^{(j)} = \int_{iT}^{(i+1)T} r(t) a_j(t) \cos(\omega_0 t + \Phi_j) dt = I_i^{(j)} + v_i + \delta_i \quad (15)$$

where $I_i^{(j)}$ is the useful component (desired contribution from user j), v_i is the multiple access interference from the other $(K-1)$ users and δ_i is the noise contribution. Considering the Euclidian normalization, $I_i^{(j)}$ is given by,

$$I_i^{(j)} = \sqrt{2} P_j m_{j,i} \int_i^{(i+1)T} a_j^2(t) \cos^2(\omega_0 t + \Phi_j) dt$$

$$I_i^{(j)} = \sqrt{\frac{P_j}{2}} m_{j,i} T \quad (16)$$

where $m_{j,i}$ is data of the j^{th} user at the end of the i^{th} bit period T . T is the period of the symbols, P_j is the received power of user j.

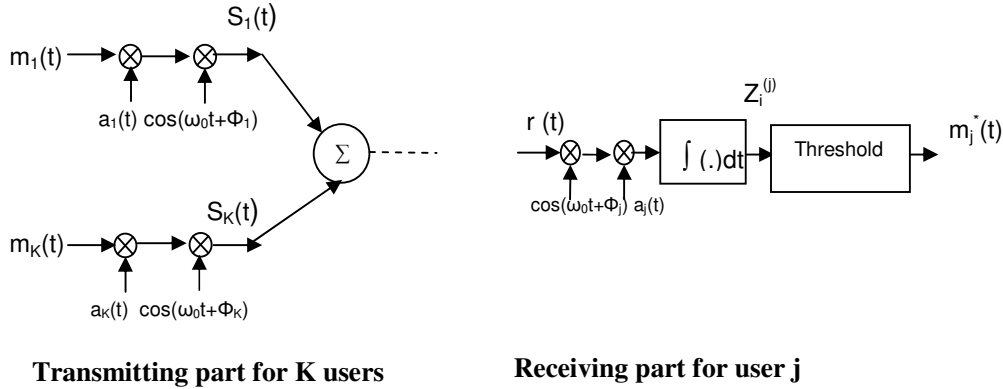


Figure 2. A simplified diagram of a CDMA system

In [22] it is shown that for a synchronous system that assumes synchronized spreading sequences and constant power levels for all K users $P_i = P_j$ at the receiving part, dependency of the average BER on the white noise PSD and Multiple Access Interference (MAI) power is given by,

$$P_e = Q \left(\sqrt{\frac{2E_b/N_0}{1 + \frac{K-1}{N^2} C^2 E_b/N_0}} \right) \quad (17)$$

Where $E_b = P_j T$ is the signal energy per bit period, E_b/N_0 is the signal-to-noise ratio expressed in dB, K is number of users, C^2 is the mean square cross-correlation value and N is the length of the spreading sequence.

$$\sum_{l=1}^N a_j(l) a_k(l) = C_{j,k}^{(l)} \quad (18)$$

Equation (18) represents the cross-correlation function of the two sequences $\{a_j(l)\}$ and $\{a_k(l)\}$ on the i^{th} bit period.

The CCR values between two sequences of same length depend on the two sequences considered and the shift. Smaller the CCR values better the immunity against MAI. To study the performance, the peak pairwise CCR value α is considered and with reference to this corresponding BER is computed.

$$\text{Here } C = \max_i [C^{(i)}_{j,k} \text{ for all } j, k] \quad (19)$$

For Gold sequences of 63 bits the pairwise CCR value α is less than or equal to 0.2698 and there are 65 Gold sequences. But using the proposed scheme there are sequences of 63 bits having pairwise CCR value $\alpha \leq 0.2381$ and $\alpha \leq 0.2063$. Similarly for sequences of length 127 and 255 bits, there are sequences having pairwise CCR value α which is less than that of Gold sequences. Hence to study the performance of the proposed scheme, α is considered to be worst case CCR value.

It can be seen that the average BER of a synchronous DS-CDMA system versus the number of users depends on the MAI term. The MAI contribution to BER grows with the number of simultaneous users 'K' in the system. K depends on the number of sequences having pairwise CCR value less than α , type of chaotic function and type of binary conversion. This MAI term depends proportionally on the mean square cross-correlation value $C^2 = E [(C^{(i)}_{j,k})^2]$ of the spreading sequences' set. Hence, in order to have lower BER values one has to choose sets of spreading sequences with low mean square cross-correlation values. Since α is considered to be the worst case CCR value, α^2 is computed and equated to the mean square cross-correlation value and the BER performance is investigated. Therefore equation (17) in terms of α is given by,

$$P_e = Q \left(\sqrt{\frac{2E_b/N_0}{1 + \frac{K-1}{N^2} \alpha^2 E_b/N_0}} \right) \quad (20)$$

The non-zero pairwise CCR value α considered becomes interference for other users. As a result, as the number of users increases, the BER degrades. This is shown in Figures 4 to 6. In each case the available number of code sequences is also indicated. Taking into consideration α^2 value, the BER performances given by equation (20) for the chaotic sequences generated (for six equations (4) to (9)) using polynomial mapping given by equation (1) and are compared with Gold sequences and Kasami sequences. The BER versus number of user's plots for sequence generated using polynomial mapping given by equation (1) of length 63 bits, 127 bits and 255 bits is shown in Figure 3, 4 and 5 respectively. Figures 6, 7 and 8 depict the BER versus SNR plots for the sequences of length 63 bits, 127 bits and 255 bits respectively.

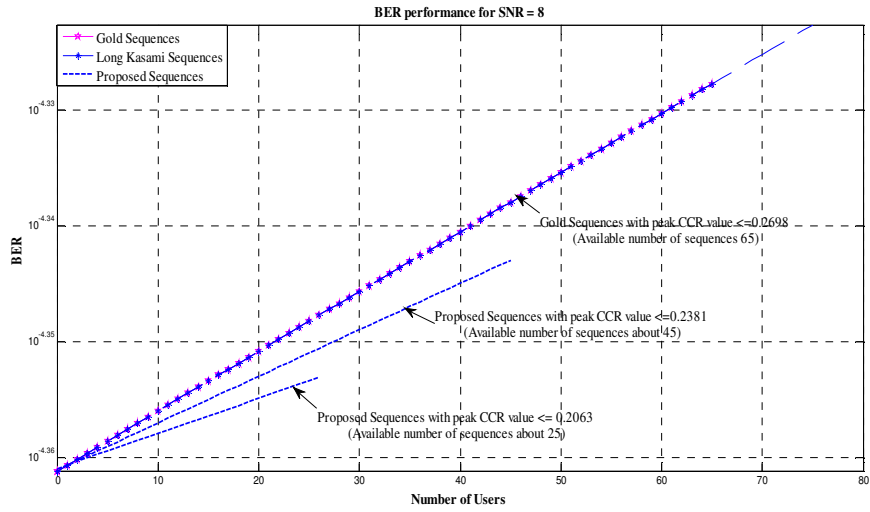


Figure 3. BER versus Number of users plot for sequence of length 63 bits

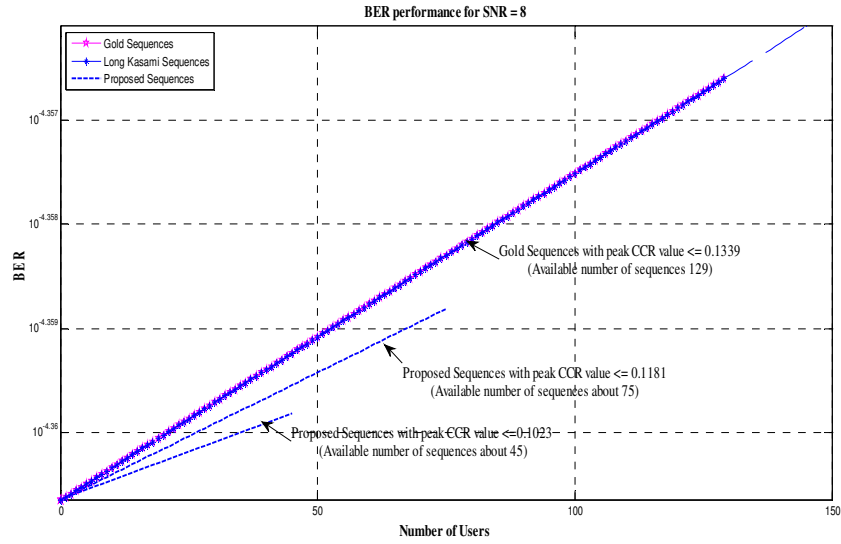


Figure 4. BER versus Number of users plot for sequence of length 127 bits

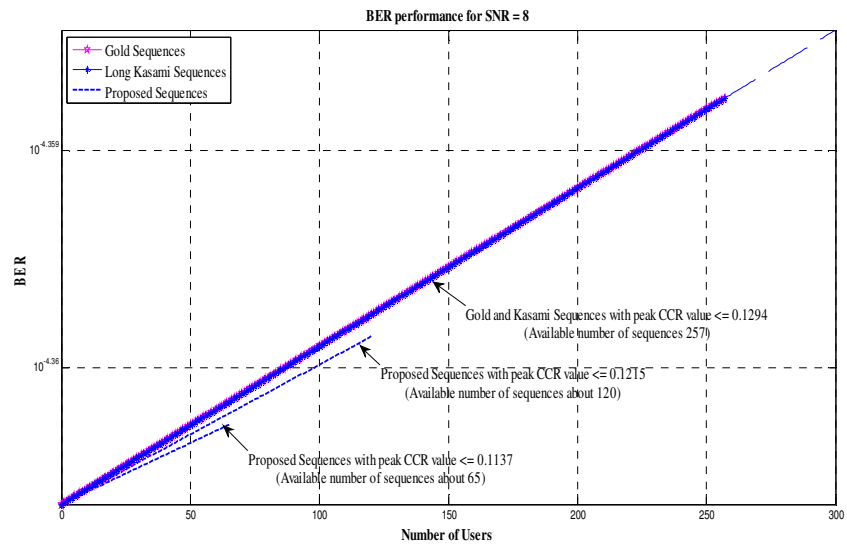


Figure 5. BER versus Number of users plot for sequence of length 255 bits

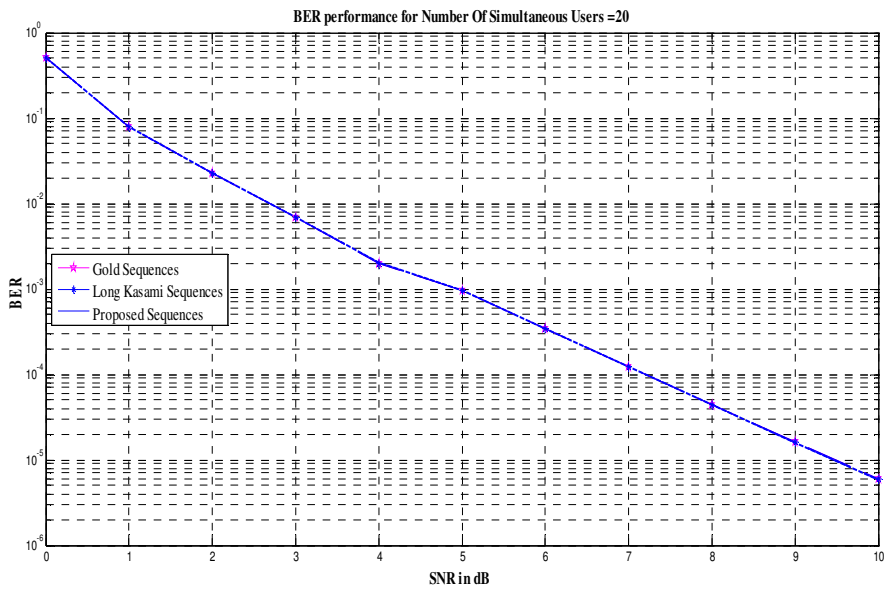


Figure 6. BER versus SNR plot for sequence of length 63 bits

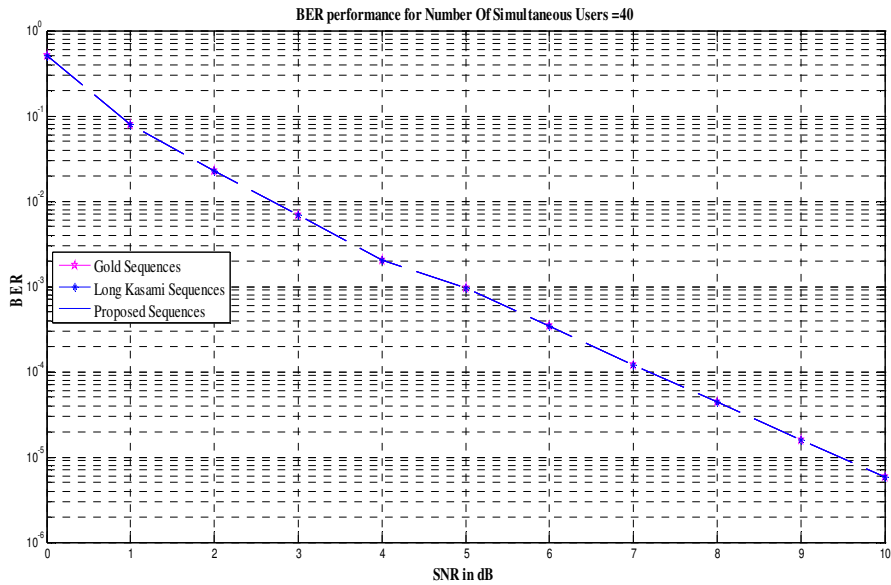


Figure 7. BER versus SNR plot for sequence of length 127 bits

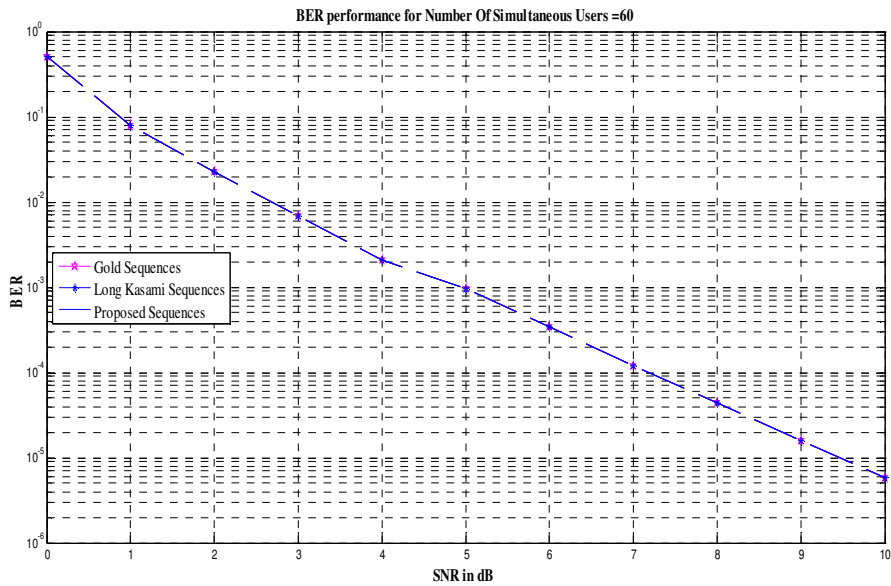


Figure 8. BER versus SNR plot for sequence of length 255 bits

In general as number of users increases BER also increases for a fixed value of SNR. However in the proposed scheme set of sequences whose pairwise CCR value α less than that of Gold sequences exhibit better BER performance. This is shown in figures 3, 4 and 5. If the number of users is fixed and pairwise CCR value α is considered to be same as that of Gold sequences, BER decreases uniformly as SNR increases in all the cases. This can be seen in Figures 6, 7 and 8.

3. CONCLUSIONS

In this paper, polynomial mapping suggested in [18], $P_f(x) = (x^2 - x) \bmod 4$ is chosen for the conversion of sequence over Z_4 to binary for the 6 chaotic map equations. Some segments of length 63, 127 and 255 bits of the generated chaotic binary sequences are tested for cross correlation and linear complexity properties. The investigation is done for segments of 63, 127 and 255 bit binary sequences for each case of $n = 5, 6, 7, \dots, 10$ and compared with Gold sequences and Kasami sequences. From the results it is observed that there are segments of 63 bit, 127 bit and 255 bit with pairwise CCR value less than that of Gold sequences. Hence using the proposed model it is possible to generate sequences with pairwise CCR value less than that of Gold sequences. The BER performance of these sequences as code sequences in CDMA is better than that of Gold and Kasami sequences.

It is seen that the sequences chosen using the proposed method have linear complexity greater than that of Gold sequences of same length.

It is shown that, there are set of sequences with peak pairwise CCR value same as that of Gold sequences. However, number of such sequences is more than that of Gold sequences.

Also there are set of sequences whose peak pairwise CCR value is less than that of Gold sequences. But the number of such sequences is less than that of Gold sequences.

However in the proposed scheme, set of sequences whose pairwise CCR value α less than that of Gold sequences exhibit better BER performance and as the number of users increases BER also increases for a fixed value of SNR. Also if the number of users is fixed and pairwise CCR value α is considered to be same as that of Gold sequences, BER decreases uniformly as SNR increases in all the cases.

ACKNOWLEDGEMENTS

The authors would like to thank the Management and Principal, Dr. Ambedkar Institute of technology, Bengaluru for providing the facilities to carry out this work. Authors also thank Dr. Ramesh S, Prof. Shivaputra and Prof. Chetan S for their valuable suggestions.

REFERENCES

- [1] K T Alligood, J A Yorke and T D Sauer, Chaos: An Introduction to Dynamical Systems, Springer-Verlag Inc., 1997.
- [2] Robert M. May, Simple Mathematical Models with Very Complicated Dynamics, Nature 261 (1976) 459–467.
- [3] Martin Hasler, and Yuri L. Maistrenko, An Introduction to the Synchronization of Chaotic Systems: Coupled Skew Tent Maps, IEEE Trans. Circuits and Systems-I: Fundamental Theory and Applications, Vol. 44, No.10 (1997) 856 – 866.
- [4] Robert M. May, Mathematical Modelling: The Cubic Map in Theory and Practice, Nature 311 (1984) 13 - 14 ; doi:10.1038/311013a0.
- [5] P. Morton, Arithmetic Properties of Periodic Points of Quadratic Maps, Acta Arithmetica (1998) 89 – 102.
- [6] Heidari-Batani G., McGillem C.D. and Tenorio M.F, A Novel Multiple-address Digital Communication System Using Chaotic Signals, Proc. International Communication Conference, Chicago, USA (1992) 1232–1236.
- [7] Zhiyu Zhang, Jiulong Zhang, Wei Xiao, Yanjun Lu, Performance Enhancement of DS/SS System Using Hybrid Chaotic Spreading Sequence, Proc. of IEEE ICCT, Guilin, China, Vol. 1(2006) 522-526.

- [8] B. Jovic, C.P. Unsworth, G.S. Sandhu and S.M. Berber, A Robust Sequence Synchronization Unit for Multi-User DS-CDMA Chaos-Based Communication Systems, *Signal Processing*, Vol. 87, Issue 7 (2007) 1692-1708.
- [9] Georges Kaddoum, Daniel Roviras, Pascal Charge and Daniele Fournier-Prunaret, Accurate Bit Error Rate Calculation for Asynchronous Chaos-Based DS-CDMA over Multipath Channel, Hindawi Publishing Corporation, *EURASIP Journal on Advances in Signal Processing*, Vol. 2009, Article ID 571307 (2009) 1-12.
- [10] Georges Kaddoum, Martial Coulon, Daniel Roviras and Pascal Chargé, Theoretical Performance for Asynchronous Multi-User Chaos-Based Communication Systems on Fading Channels, *Signal Processing*, Vol. 90, Issue 11 (2010) 2923-2933.
- [11] R. Vali, S.M. Berber and S.K. Nguang, Effect of Rayleigh Fading on Non-Coherent Sequence Synchronization for Multi-User Chaos Based DS-CDMA, *Signal Processing*, Vol. 90, Issue 6 (2010) 1924-1939.
- [12] Venkatesh S, Poonam Singh, Multi User Chaos Based DS-CDMA System Using Orthogonal Chaotic Vector, *Proc. International Conference on Electronic Systems* (2011) 339 – 342.
- [13] G. Venkat Reddy, Bibhudendra Acharya and Sarat Kumar Patra, Performance Evaluation of Different DS-CDMA Receivers Using Chaotic Sequences, *International Conference on RF and Signal Processing Systems* (2008) 426 – 431.
- [14] V.Nagarajan and P. Dananjayan, Performance Analysis of MIMO MC-DS/CDMA System using Chaotic Spreading Sequence, *Int. Jnl. of Computer and Electrical Engineering*, Vol. 2, No. 2 (2010) 329 – 333.
- [15] Mahalinga V. Mandi , K.N. Haribhat , R. Murali, Generation of Discrete Spreading Sequences using Chaotic Functions and their use in Spread Spectrum Communication, *Proc. Sonata International Conf. Computer, Communication and Controls* (2006) 128 - 133.
- [16] Mahalinga V. Mandi , K.N. Haribhat , R. Murali, Chaotic Functions for Generating Binary Sequences and their Suitability in Multiple Access, *Proc. IEEE International Conference on Communication Technology 2006 (IEEE-ICCT 2006)*, Vol. 1 (2006) 217 – 220.
- [17] Mahalinga V. Mandi, K. N. Haribhat, R. Murali, Generation of Large Set of Binary Sequences Derived from Chaotic Functions with Large Linear Complexity and Good Cross Correlation Properties, *International Journal of Advanced Engineering and Applications (IJAEA)*, Vol. III (2010) 313 – 322, ISSN: 0975 – 7783 (Print), 0975 – 7791 (Online).
- [18] P. Udaya and M.U Siddiqi, Optimal Biphasic Sequences with Large Linear Complexity Derived from Sequences Over Z₄, *IEEE Trans. Information Theory*, Vol. 42, No. 1 (1996) 206 – 216.
- [19] Abraham Lempel and Haim Greenberger, Families of Sequences with Optimal Hamming Correlation Properties, *IEEE Trans. on Information Theory*, Vol. IT-20, No.1 (1974) 90-94.
- [20] J.L. Massey, Shift Register Synthesis and BCH Decoding, *IEEE Trans. Information Theory*, Vol. IT-15 (1969) 122-127.
- [21] Robert Gold, Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions, *IEEE Trans. on Information Theory*, (1968) 154 – 1556.
- [22] C. Vladeanu and I. Banica, Performance of Iterative Multistage Detectors for DS-CDMA Systems, *Proc. of IEEE-ICT 2001* (2001) 35-39.

Authors

Mahalinga V. Mandi received the B.E. Degree in Electronics and Communication Engineering from Mysore University, Karnataka, India in 1990, M.Tech Degree in Industrial Electronics from Mysore University, Karnataka, India in 1998 and Ph.D Degree from Dr MGR University, Chennai, India in 2013. He is working as Associate Professor in the Department of Electronics & Communication Engineering, Dr Ambedkar Institute of Technology, Bangalore, India. His research areas include Digital Communication, Cryptography and Network Security and Digital Signal Processing.



Dr K N Haribhat received the B.E Degree with honors from Mysore University in 1966, M.Tech and Ph.D in Electronics & Communication Engineering from Indian Institute of Technology, Kanpur, in 1973 and 1986, respectively. He is Dean Academic and Head (Retired), Department of Electronics & Communication Engineering at Nagarjuna College of Engineering & Technology, Bangalore, India. He was with Karnataka Regional Engineering College, Suratkal, India (Currently known as NIT-K) for more than 30 years. His research areas include Analog Communication, Digital Communication and Cryptography. He has authored more than 25 papers in National/international Conferences and Journals. He has coauthored three books on communication.



Dr Murali R received the M.Sc Degree in Mathematics from Bangalore University, Karnataka, India in 1990 and Ph.D Degree in Mathematics from Bangalore University, India in 1999 and currently working as Professor in the Department of Mathematics, at Dr Ambedkar Institute of Technology, Bangalore, India. His research areas include Graph Theory-Hamiltonian graphs. He has authored more than 20 papers in National/International Journals.

