Available online at www.sciencedirect.com

ScienceDirect

IERI Procedia 4 (2013) 309 – 315

Procedia IERI

www.elsevier.com/locate/procedia

2013 International Conference on Electronic Engineering and Computer Science

Blum BlumShub Pseudorandom Sequence based Peak Power Control in MC-CDMA System

Noor Mohammed V[a*], P.S. Mallick[a], L.Nithyanandan[b], Mohit Asrani[a],Mayank Saxena[a]

[a]*VIT University, Vellore, Tamil Nadu, India.*
[b] *Dept. of ECE,Pondicherry Engineering College, Pondicherry, India.*

Abstract

This paperanalyses thePeak to Average Power Ratio (PAPR) for various sequences such as Walsh Hadamard (WH), Gold Sequence,Welch-Gong(WG)sequence and Blum BlumShub (BBS) sequence in Multicarrier Code Division Multiple Access(MC-CDMA)system. Inmultiuser MC-CDMA system, the Blum BlumShub(BBS) sequence provides reduced peak to mean envelope power ratio(PMEPR)when comparedto WH sequence. So,this BBS sequence can be considered as a good alternative for Walsh Hadamard (WH) sequence in reducing PAPR in MC-CDMA system.

Selection and peer review under responsibility of Information Engineering Research Institute

*Keywords:*Blum Blum Shub(BBS) Sequence ; Gold Sequence ;MC-CDMA; PAPR; Walsh Hadamard(WH); WG Sequence.

1. Introduction

Today is the time of fast communication, where every communication system is going mobile and wireless,so there is a need to develop a system which will prevent the power loss and interference from the system for faithful data transmission. For high data transmission in most of the communication system, a concept is introduced-MC CDMA[1], which is a mixture of Orthogonal frequency division Multiplexing (OFDM) and Code division Multiple Access (CDMA). This MC-CDMA system is immune to multipath

* Corresponding author. Tel.:+91-9786340547
E-mail address: vnoormohammed@vit.ac.in

2212-6678
Selection and peer review under responsibility of Information Engineering Research Institute
doi:10.1016/j.ieri.2013.11.044

fading and narrow band interference on one hand, and provides high data rate on other hand. Although, there is high data rate transmission and immunity from multi path fading, the major problem of MC-CDMA system is that it suffers from high Peak to Average Power Ratio(PAPR). The main advantage of MC-CDMA over single carrier scheme is the ability to cope up with several channel conditions, such as, frequency selective fading caused by multipath and narrow band interface. Using IFFT/FFT techniques in modulation and demodulation, high computational speed can be achieved. One way to reduce the PAPR is using codes or sequences. InMC-CDMA system with single user scenario the crest factors (CF)-$\sqrt{PAPR}$ of different codes has been explained[2]. In MC-CDMA system with multiuser scenario[3] the CFs of different spreading codes[4] have been analyzed.Using Walsh and Golay complementary sequences[5] they have analyzed the downlink MC-CDMAPAPR properties in multiuser scenario. Stillexploration for better codes with low PAPR is in initial phase.

Binary sequences are used in cryptosystems and spread spectrum communication[10]. Those binary sequences have good autocorrelation properties[6].This paper analyses the PAPR for various sequences such as Walsh Hadamard (WH), Gold Sequence, Welch-Gong(WG) sequence and Blum BlumShub (BBS) sequence in MC-CDMA system.From the simulation results it is illustrated that the BBS sequences provide improved PAPR property.

2. MC-CDMA System Model

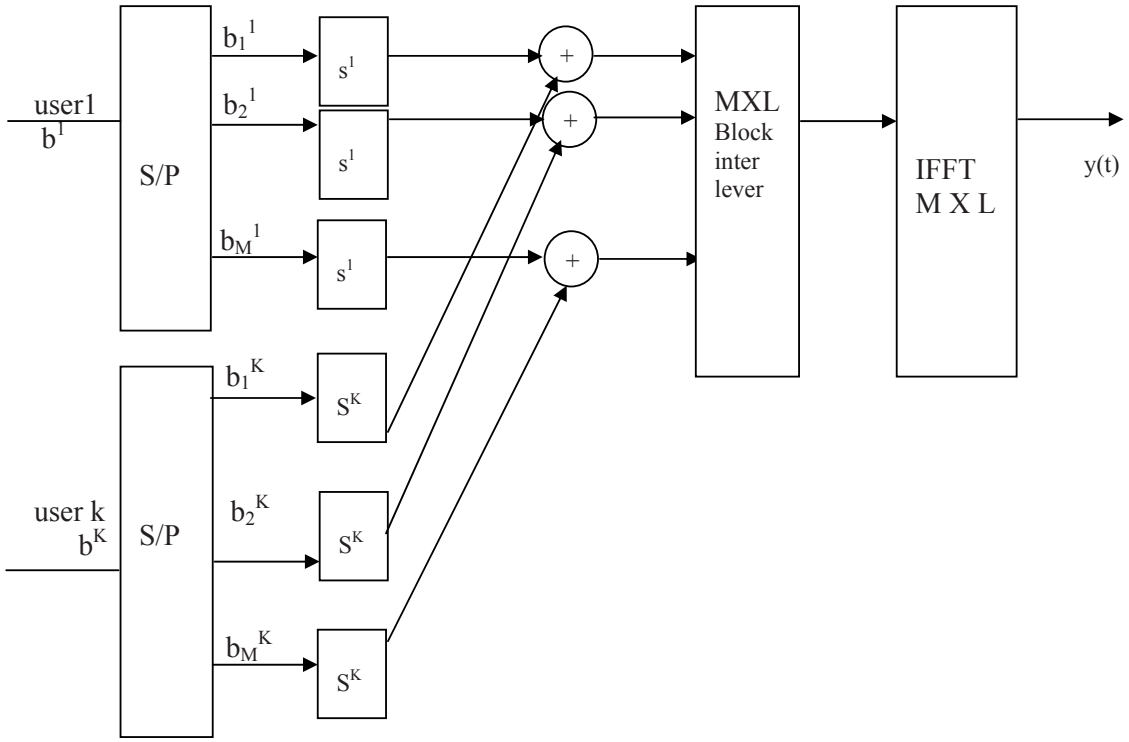

Fig1.MC-CDMA transmitter

Fig.1illustratesthe MC-CDMA transmitter, with length of spreading codes denoted by N and number of users by M, such that,M≤N. The user data symbol is represented by K. The m^{th} user is represented as $b^m=[b_1^m, b_2^m, \ldots . b_K^m]$. The corresponding spreading sequence for the m^{th} user is $s^m = [s_1^m s_2^m, \ldots . s_N^m]$. The first stage of the transmitter which is user data symbols M arespreaded and thenadded. The second stage is the added user symbols are interleaved. The final stage is the Inverse Fast Fourier Transform (IFFT). The IFFT input is interleaved user data symbol. The size of the IFFT is L=KXN. The subcarrier is denoted by L. The transmitter signal can berepresented asfollows [10]

$$y(t) = \sum_{l=0}^{L-1} \sum_{m=1}^{M} b_k^m s_n^m e^{j2\pi lt/Ts} \quad 0 \le t \le T_s \tag{1}$$

Symbol period is Ts.

The PAPR of y(t) as follows

$$y(t)=\max|R(y(t))|^2/1/T_s\int|y(t)|^2dt \tag{2}$$

Here$R$(.) is the real part of the variable. It is forthright that in [9]

$$PAPR \le PMEPR=\max\ 0 \le t \le Ts\ |y(t)|^2 / (1/T_s)\int_0^{Ts} |y(t)|^2 dt \tag{3}$$

There are various sequences used for spreading the data. In this paper, the spreadingsequences used areWalsh Hadamard(WH),Gold Sequence,WG Sequences,Blum BlumShub sequence.

3. Set of Sequences

3.1. Walsh Hadamard Sequence

Walsh Hadamard sequence is a spreading sequence, in the form of a square matrix, with dimension power of 2.The entries of Walsh Hadamard matrix are either +1or -1.It satisfies the property that, for any two column or row thedot product is always zero. Each row of a Walsh matrix corresponds to a Walsh function .Walsh matrix [1] is given by $H(2^n)$,where n is any natural number.

In general,

$$\begin{bmatrix} H(2^n) = H_{2(n-1)} & H_{2(n-1)} \\ H2(n-1) & -H2(n-1) \end{bmatrix} \tag{4}$$

3.2. Gold Sequence

Gold code, otherwise called as Gold sequencesis generated by Gold code generator, which is a combination of two Pseudo Noise(PN) Sequence.These codes form a family of codes, called as quadratic form sequences. This Gold code is a binary sequence. They have got a property of smaller cross-correlation[7] in a set, which are very use full, when multiple signals are broadcasted at same frequency.

Algorithm for generating Gold code

(1)Select s={s(t) } and r={r(t)},be any sequences, with period $n=2^m-1$.

(2)Take modulo 2 sum of s, with n cyclic shifted version of r.

(3) By this, a new sequence is obtained, with period 'n'.

If original sequences, s and r are also included, total number of sequences is n+2.Resulted sequence obtained is called Gold code or Gold sequences.

3.3. Welch-Gong Sequence

The WG sequence construction procedure is specified in [8]. Let m (mod 3)≠0, the primitive element of GF(2^m) is α , the trace representation is given by $a_u = \sum_{u \varepsilon I} Tr\ (\alpha^u)$where I refers to the set of trace exponents which is defined in [8]. The trace exponent of WG sequences [10] for m=7 and 8 is shown in Table.1

Table.1 Trace exponent of WG sequences

M	WG Sequences
7	1,3,7,9,29
8	19,39,13,21,29

3.4.BLUM BLUM SHUB Sequence

Blum BlumShub (BBS) [11] is a pseudorandom bit generator, instead of pseudorandom number generator, generating binary sequence,called as Blum BlumShub sequences. The following steps are taken to generate the BBS sequences

(1)Find two prime numbers p and q in the form of 4k+3,where k is any integer (both the prime number p and q are congruent to 3 modulo 4)

(2)Select,the modulus n=pxq

(3)Choose a random integer 'r',which is co- prime to n

(4)For first iteration, select $x_0=r^2 \bmod n$,(this x_0 is called as seed)

(5)Generating sequence by $X_{n+1}=(x_n)^2 \bmod n$

To get the random bit in binary form, convert all the decimal digit into binary form andtake the LSB of it, and represent 1 as 1 ,and 0 as -1.This sequence of 1 and -1,are used as spreading sequences .

.

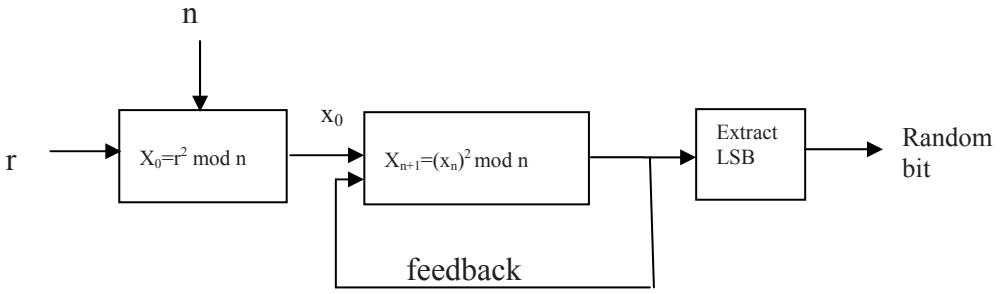

Fig.2.Block diagram for Blum BlumShub sequence generator

4. Simulation Results

In the results, properties of PAPR in multiuser MC-CDMA system with different sequencesare discussed.In multi user scenario the PMEPRcan be modified based on the system model.

$$\text{PMEPR} = \max 0 \le t < T_s |y(t)|^2 / \sum_{l=0}^{L-1} | \sum_{m=1}^{M} b_k^m s_n^m |^2 \quad (5)$$

In the simulation, the system parameters are as follows: In WG sequence for the primitive polynomials generating finite field GF(2^m), m=7 for the binary sequences. In BBS sequences the p=17, q=23 and r=19. In

fig.3 128 subcarrier where L=128 and K=1and fig. 4, 256 subcarrier where L=128 and K=2. Table2 shows the theoretical comparison of the PMEPR for four different spreading codes(parameters related to Fig.4).Generally, if thenumber of users are large,it is observed thatspreading code can aid to reduce the PAPR. The results show thatBBS sequences can be viable alternative to traditional Walsh Hadamard (WH) spreading sequences for reduced PAPR in MC-CDMA.

Table.2Comparison of PMEPR, using different spreading sequences, for multiple users .

No.of users	Walsh Hadamard	Gold Sequence	WG Sequence	Blum BlumShub
5	11.84	11.52	11.52	9.5
10	8.95	8.5	8.5	6.5
15	6.6	6.676.6		4.75
20	5.7	5.5	5.5	3.5
25	4.86	4.5	4.5	2.6
30	4.09	3.7	3.7	1.7

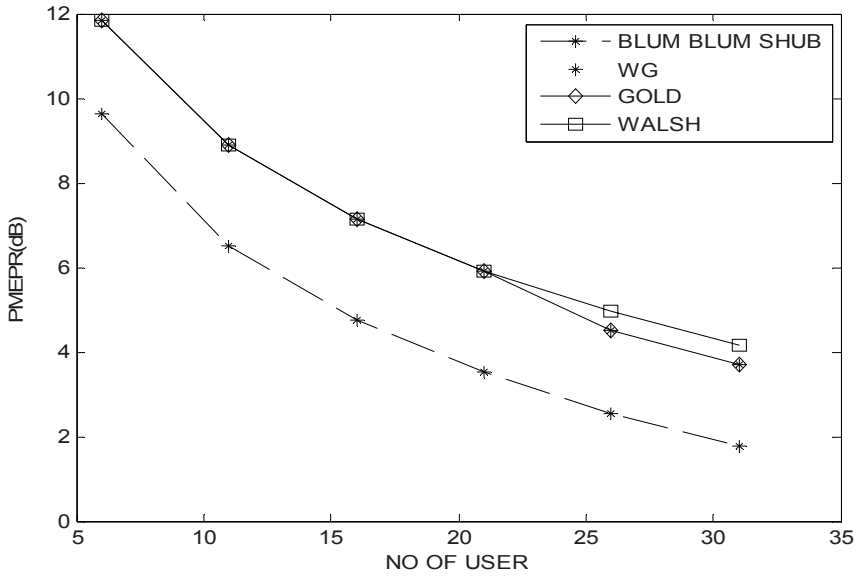

Fig3. PMEPRof multiple users M with N=128,K=1 and L=128.

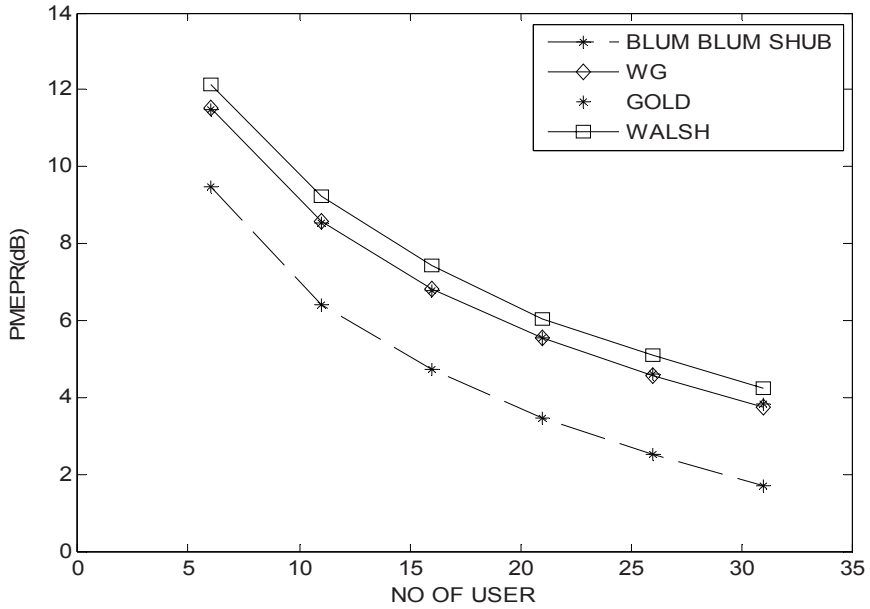

Fig4. PMEPR of multiple users M with N=128,K=2 and L=256.

5. Conclusion

In this paper the PAPR in MC-CDMA system using different spreading sequences are investigated.For multiple users,PMEPR values are high in Walsh Hadamard sequences,whereas in Gold sequences and WG sequences the PMEPR values are relatively equal but lower than Walsh Hadamard sequences. In BBS sequences the PMEPR values are lower than all the three sequences.So, it is seen that, for PAPR reduction in MC-CDMA system the BBS sequence can be effectively used as a spreading sequence.

Reference

[1] S. Hara and R. Prasad.Overview of multicarrier CDMA.IEEE Communication Magazine,1997:128-133.
[2] B. M. Popovi´c.Spreading sequences for multicarrier CDMA systems. IEEE Trans. Commun.1999;47(6): 918-926.
[3] Choi B J, Tellambura C and Hanzo L.Crest Factors of Shapiro-Rudin Sequence Based Multi-Code MC-CDMA Signals.VTC'2002 (Spring),2002:1472-1476.
[4] L. Hanzo, M. Munster, B. J. Choi, and T. Keller,OFDMand MC-CDMA for Broadband Multi-user Communications,WLANs and Broadcasting.IEEE Press. 2003.
[5] HidekiOchiai, Hideki Imai.Performance of OFDM-CDMA with Simple Peak Power Reduction.European Transactions on Telecommunications.1999;10(4):391–398.
[6] Alvy Ray Smith.General Shift register sequence of arbitrary cycle length.IEEE Transaction Computers. 1997;C-20(4):456-459.
[7] S. W. GolombShift Register Sequences.Aegean Park Press Laguna Hills.1981.
[8] Solomon W. Golomb.Signal Design for Good Correlation,For Wireless Communication, Cryptography,

and Radar, Cambridge University Press. 2005
[9] S. Litsyn. Peak Power Control in Multicarrier Communications,Cambridge University Press, 2007.
[10] XinGao, Nam Yul Yu, Zhiwei Mao. Peak Power Control of MC-CDMA with special classes of binary sequences.Electrical and Computer Engineering (CCECE) 23rd Canadian conference.2010; 1-4.
[11]. William Stallings.Cryptography and Network Security.Fourth Edition.PHI, 2006.