# Cryptographic Functions and Bit-Error-Rate Analysis with Almost $p$-ary Sequences

Büşra Özden, Oğuz Yayla

Department of Mathematics, Hacettepe University, Ankara, Turkey,
E-mail: {*busra.ozden,oguz.yayla*}*@hacettepe.edu.tr*

ORCID ID: 0000-0002-1692-5441, 0000-0001-8945-2780

Research Paper Received: 06.08.2019 Revised: 05.09.2019 Accepted: 11.09.2019

**Abstract**—Sequences are used for achieving non-linearity in a cryptosystem, and they are important in Code Division Multiple Access (CDMA) to ensure a proper communication. In this study, we show a method for obtaining cryptographic functions from $p$-ary sequences with $s$ consecutive zero-symbols of type $(\gamma_1, \gamma_2)$. In fact, most of the cases we obtain functions with the highest non-linearity, i.e. generalized bent functions. In CDMA, instead of distributing time and frequency sources to users, each user is given a unique sequence to transmit data at the same frequency and time. In this study, we examined the bit-error-rate (BER) performance of $p$-ary sequences with $s$ consecutive zero-symbols of type $(\gamma_1, \gamma_2)$ on CDMA.

**Keywords**—nearly perfect sequences, cryptographic functions, generalized bent function, CDMA, bit-error-rate.

## 1. Introduction

Sequences are applied in many practical areas, for example, satellite telecommunication, cryptographic function design, wireless networks, radar systems, and modern cell phones (see [1], [5], [6], [7], [8]).

In cryptography, non-linearity is satisfied by substitution boxes (s-boxes) because they confuse a message into a cipher-text. Maximum non-linearity is obtained by so called bent functions used in the s-boxes. It is well known that one can get a generalized bent function from a perfect sequence (see [1] or Theorem 1 below). In this study, we use this connection and convert a nearly perfect sequence of type $(\gamma_1, \gamma_2)$ to a generalized bent function in Section 4 and also we tabulate the examples of Walsh spectrum of functions obtained from nearly perfect sequences of type $(\gamma_1, \gamma_2)$ (see Table 1). It is seen that generalized bent functions can be obtained from nearly perfect sequences, and we obtain a larger set of cryptographic functions with the similar properties of generalized bent functions.

In Code Division Multiple Access (CDMA), sequences with ideal autocorrelation are important because a signal should not be affected by other signals in order to provide high-quality communication. For this reason, sequences with the ideal autocorrelation have been studied by many authors [9]-[11]. Initially, binary sequences were widely studied, but complex sequences were started to be studied over time due to the lack of binary sequences with the ideal autocorrelation. In this study, $p$-ary sequences with $s$ consecutive zero-symbols of type $(\gamma_1, \gamma_2)$ and their applications to the bit-error-rate (BER) on CDMA are presented. The simulation results on BER analysis of CDMA with almost $p$-ary nearly perfect sequence is given in Section 5. It is seen that although almost $p$-ary nearly perfect sequences don't have better simulation results than perfect sequences, they serve a large set of sequences with almost ideal autocorrelation coefficients.

The rest of this paper is organized as follows. In Section 2, we give some of the necessary definitions of $p$-ary sequences. In Section 3, we define $(\gamma_1, \gamma_2)$-near Butson-Hadamard (resp. Conference) matrix (see Definition 2). In Section 4, the equivalence between an almost $p$-ary nearly perfect sequence of type $(\gamma_1, \gamma_2)$ and a $(\gamma_1, \gamma_2)$-near Conference matrix and a cryptographic function is studied and some examples of cryptographic function are presented (see Table 1). In Section 5, we study CDMA structure on the Rayleigh channel under additive white Gaussian noise (AWGN) as a communication application (see Figure 1), and we use the almost $p$-ary sequences in this scenario. On this structure, bit-error-rate is calculated and simulation results are given (see Figures 2-5).

## 2. Preliminaries

Let $\zeta_p \in \mathbb{C}$ be a primitive $p$-th root of unity for some prime number $p$. A sequence $\underline{a} = (a_0, a_1, \ldots, a_{n-1}, \ldots)$ of period $n$ with $a_i = \zeta_p^{b_i}$ for some integer $b_i$, $i = 0, 1, \ldots, n-1$ is called a *$p$-ary sequence*. If $a_{i_j} = 0$ for all $j = 1, 2, \ldots, s$ where $\{i_1, i_2, \ldots, i_s\} \subset \{0, 1, \ldots, n-1\}$ and $a_i = \zeta_p^{b_i}$ for some integer $b_i$, $i \in \{0, 1, \ldots, n-1\} \backslash \{i_1, i_2, \ldots, i_s\}$, then we call $\underline{a}$ an *almost $p$-ary sequence with $s$ zero-symbols*. For instance, $\underline{a} = (\zeta_3^3, \zeta_3^2, \zeta_3^4, \zeta_3^2, 1, \ldots)$ is a 3-ary sequence of period 5 and $\underline{a} = (0, \zeta_7^3, 1, \zeta_7^3, 0, 0, \zeta_7^5, \zeta_7^6, \zeta_7^6, \zeta_7^5, , \ldots)$ is a 7-ary sequence with 3 zero-symbols of period 10. It is widely used that a sequence with one zero-symbol is called an almost $p$-ary sequence [4]. But in this paper we use this notation for a $p$-ary sequence with $s$ zero-symbols, for $s \geq 0$.

For a sequence $\underline{a}$ of period $n$, its *autocorrelation function $C_{\underline{a}}(t)$* is defined as

$$C_{\underline{a}}(t) = \sum_{i=0}^{n-1} a_i \overline{a_{i+t}},$$

for $0 \leq t \leq n-1$ where $\overline{a}$ is the complex conjugate of $a$. The values $C_{\underline{a}}(t)$ at $1 \leq t \leq n-1$ are called *the out-of-phase autocorrelation coefficients* of $\underline{a}$. Note that the autocorrelation function of $\underline{a}$ is periodic with $n$.

We call an almost $p$-ary sequence $\underline{a}$ of period $n$ a *nearly perfect sequence* (NPS) of type $(\gamma_1, \gamma_2)$ if all out-of-phase autocorrelation coefficients of $\underline{a}$ are either $\gamma_1$ or $\gamma_2$. According to [3, Theorem 2], we know that

$$C_{\underline{a}}(t) = \begin{cases} \gamma_1 & \text{if } t = 1, n-1, \\ \gamma_2 & \text{if } t = 2, 3, \ldots, n-2. \end{cases}$$

We write *NPS of type $\gamma$* to denote an NPS of type $(\gamma, \gamma)$. Moreover, a sequence is known as *perfect sequence* (PS) if it is an NPS of type $(0, 0)$, therefore the concept of NPS is a generalization of PS. For instance, $\underline{a} = (0, 0, \zeta_3, \zeta_3, \zeta_3, \ldots)$ is an almost 3-ary NPS of type (2,1). On the other hand, $(1, \zeta_3, \zeta_3, \ldots)$ is a 3-ary NPS of type (0,0) and period 3, in fact this is a PS.

## 3. Butson-Hadamard Matrices

We first give the definition of a Butson-Hadamard matrix and a near Butson-Hadamard matrix.

A Hadamard matrix is an $(v \times v)$ matrix with entries in $\mathbb{Z}_2$ such that $HH^T = vI$. A square matrix $H = (h_{ij})$ of order $v$ is called $circulant$ if $h_{i+1,j+1} = h_{i,j}$ for all $0 \leq i, j < v$.

$$A = \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}, \quad B = \begin{bmatrix} - & 1 & 1 & - & - \\ - & - & 1 & 1 & - \\ - & - & - & 1 & 1 \\ 1 & - & - & - & 1 \\ 1 & 1 & - & - & - \end{bmatrix}$$

In the above examples, the matrix $A$ is a Hadamard matrix of order 2 and the matrix $B$ is a circulant matrix of order 5, where $-$ represents $-1$. Let $p$ be a prime and $\mathcal{E}_p = \{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$ where $\zeta_p = e^{\frac{2i\pi}{p}}$. The identity matrix is denoted by $I$ and all one matrix denoted by $J_1$. Moreover, $J_2$ and $J_3$ are defined as

$$J_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix},$$

$$J_3 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & \dots & 1 & 1 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \vdots \\ 1 & 1 & 1 & 0 & 0 & \dots & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & \dots & 0 & 0 \end{bmatrix}.$$

So, $J_1 = J_2 + J_3 + I$.

*Definition 1:* A Butson-Hadamard matrix is a square matrix $H$ of order $v$ with entries in $\mathcal{E}_p$ such that $H\bar{H}^T = vI$, where $\bar{H}$ denotes the complex conjugation of each entries of $H$. It is denoted by $BH(v, p)$. $BH(v, 2)$ is so called Hadamard matrix of order $v$. A $\gamma$-near Butson-Hadamard matrix is an $(v \times v)$ square matrix with entries in $\mathcal{E}_p$ such that $H\bar{H}^T = (v - \gamma)I + \gamma J_1$ for $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_p]$ and denoted by $BH_\gamma(v, p)$. The analysis of $\gamma$-near Butson-Hadamard matrices is given in [2].

*Example 1:* The following matrix $H$ is an $BH_\gamma(5, 5)$ for $\gamma = -\zeta_5^3 - \zeta_5^2 + 2$, where $\zeta_5$ is a 5-th root of unity,

$$H = \begin{bmatrix} 1 & 1 & -\zeta_5^2 & 1 & 1 \\ 1 & 1 & 1 & -\zeta_5^2 & 1 \\ 1 & 1 & 1 & 1 & -\zeta_5^2 \\ -\zeta_5^2 & 1 & 1 & 1 & 1 \\ 1 & -\zeta_5^2 & 1 & 1 & 1 \end{bmatrix}.$$

We extend Definition 2 given for $\gamma$-near Butson-Hadamard matrices to $(\gamma_1, \gamma_2)$-near Butson-Hadamard matrices and near Conference matrices in the following.

*Definition 2:* A $(\gamma_1, \gamma_2)$-near Butson-Hadamard matrix is a square matrix $H$ of order $n+2$ with entries in $\mathcal{E}_p$ such that $H\bar{H}^T = (n+2)I + \gamma_1 J_2 + \gamma_2 J_3$, and denoted by $BH_{(\gamma_1,\gamma_2)}(n + 2, p)$. Similarly, a $(\gamma_1, \gamma_2)$-near Conference matrix is a square matrix $C$ of order $n + 2$ with entries in $\mathcal{E}_p \cup \{0\}$ such that $C\bar{C}^T = nI + \gamma_1 J_2 + \gamma_2 J_3$, and denoted by $C_{(\gamma_1,\gamma_2)}(n + 2, p)$.

In this paper, we study only circulant $(\gamma_1, \gamma_2)$-near Conference matrices with two leading zero entries. Please note that this kind of matrices are equivalent to nearly perfect sequences of type $(\gamma_1, \gamma_2)$ by setting the first row of the matrix with the sequence itself.

*Example 2:* The following matrix

$$C = \begin{bmatrix} 0 & 0 & \zeta_5 & \zeta_5^2 & \zeta_5 \\ \zeta_5 & 0 & 0 & \zeta_5 & \zeta_5^2 \\ \zeta_5^2 & \zeta_5 & 0 & 0 & \zeta_5 \\ \zeta_5 & \zeta_5^2 & \zeta_5 & 0 & 0 \\ 0 & \zeta_5 & \zeta_5^2 & \zeta_5 & 0 \end{bmatrix}$$

is an $C_{(\gamma_1,\gamma_2)}(5, 5)$ for $\gamma_1 = \zeta_5^2 + \zeta_5^3$, $\gamma_2 = 1$ with

$|\gamma_1| \approx 1.61$, $|\gamma_2| \approx 1$. Therefore, it satisfies

$$C\bar{C}^T = 3\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix} + (\zeta_5^2+\zeta_5^3)\begin{bmatrix}0&1&0&0&1\\1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\\1&0&0&1&0\end{bmatrix}$$
$$+1\begin{bmatrix}0&0&1&1&0\\0&0&0&1&1\\1&0&0&0&1\\1&1&0&0&0\\0&1&1&0&0\end{bmatrix}$$

## 4. Generalized Bent Functions

In this section, we give a method for obtaining a generalized bent function from an almost $p$-ary NPS with two zero symbols. Before that we will give the definition of a Walsh transform, because the non-linearity of a function can be calculated by its Walsh spectrum. Then we will give the definition of generalized bent function. Let $q$ be power of a prime number $p$. For $X, Y \in (\mathbb{Z}_p)^n$, the *dot product* or *scalar product* of two vectors $X = [x_1, x_2, \ldots, x_n]$ and $Y = [y_1, y_2, \ldots, y_n]$ is defined by $\sum_{i=1}^n x_i y_i \mod p$ and denoted by $\langle X, Y\rangle$. The non-linearity of a Boolean function is the minimum of its distance from all affine functions

$$nl(f) = \min\{d(f, A_n)\},$$

where $A_n$ is the set of all affine functions in all Boolean functions of $n$ variables. Let $F(x) = (-1)^{f(x)}$, then

$$\begin{aligned}\hat{F}(x) &= \sum_{y\in(\mathbb{Z}_2)^n} (-1)^{\langle x,y\rangle}(-1)^{f(x)}\\ &= \sum_{f(x)=\langle x,y\rangle} 1 - \sum_{f(x)\neq\langle x,y\rangle} 1\\ &= 2^n - 2d(f, \langle x, y\rangle).\end{aligned}$$

So, $d(f, \langle x, y\rangle) = 2^{n-1} - \frac{1}{2}\hat{F}(x)$ is obtained. Hence, the nonlinearity of a Boolean function f on $\mathbb{Z}_2$ is $nl(f) = 2^{n-1} - \frac{1}{2}\max\{|\hat{F}(x)| : x \in \mathbb{Z}_2^n\}$.

*Definition 3:* [1] Let $F$ be functions such that $F : (\mathbb{Z}_q)^n \to \mathbb{C}$. The Walsh transform $\hat{F} : (\mathbb{Z}_q)^n \to \mathbb{C}$ of $F$ is defined by

$$\hat{F}(x) = \sum_{y\in(\mathbb{Z}_q)^n} \zeta_q^{\langle x,y\rangle} F(y)$$

for all $x \in (\mathbb{Z}_q)^n$.

*Definition 4:* [1] Let $f$ be a function such that $f : (\mathbb{Z}_q)^n \to \mathbb{Z}_q$, and $F : (\mathbb{Z}_q)^n \to \mathbb{C}$ be defined by

$$F(x) = \zeta_q^{f(x)}$$

for all $x \in (\mathbb{Z}_q)^n$. If $|\hat{F}(x)| = q^{n/2}$ for all $x \in (\mathbb{Z}_q)^n$ then $f$ is called *a generalized bent function (GBF).*

In Theorem 1, a well known connection between Butson-Hadamard matrices and generalized bent functions is given.

*Theorem 1:* [1] Suppose $f$ and $F$ are defined as above. Define the matrix $H_f = (h_{x,y})$ and $h_{x,y} = F(x - y)$ for all $x, y \in (\mathbb{Z}_q)^n$. Then, $f$ is a generalized bent function if and only if $H_f$ is a Butson-Hadamard matrix.

Now we examine the functions corresponding to almost $p$-ary NPS of type $(\gamma_1, \gamma_2)$. Note that in Theorem 1, only the first row of a BH matrix is enough to obtain the truth-table of a function. Hence we can convert a sequence into a function's truth-table. However, since we work $p$-ary sequence of type $(\gamma_1, \gamma_2)$ and period $n+2$ with two consecutive zero-symbols, we can not directly obtain the truth-table values. Thus, we first interpolate the function $f$ of largest degree from an almost $p$-ary NPS except two zero symbols. Then we get the truth-table, and so the Walsh transform of $f$ is calculated by Definition 3.

*Example 3:* We choose a NPS $\underline{a} = (0, 0, \zeta_5, \zeta_5^2, \zeta_5, \ldots)$. We look for a function $f : \mathbb{Z}_5 \to \mathbb{Z}_5$. We first set $f(3) = 1$, $f(2) = 2$ and $f(1) = 1$ by using the direction of Theorem 1. By interpolating the function $f$ of degree 2, we

TABLE 1
Examples of Walsh spectrum of some NPSs of type $(\gamma_1, \gamma_2)$

| $Sequence$ | $q$ | $\gamma_1, \gamma_2$ | $f(x)$ | $Truthtable$ | $\lvert\hat{F}\rvert$ | $GBF$ |
|---|---|---|---|---|---|---|
| $(0,0,\zeta_5^2,\zeta_5^3,\zeta_5^2)$ | 5 | $\gamma_1 = -\zeta_5^3 - \zeta_5^2 - 1, \gamma_2 = 1$ | $4x^2+4x+4$ | $(4,2,3,2,4)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5^2,\zeta_5^4,\zeta_5^2)$ | 5 | $\gamma_1 = \zeta_5^3 + \zeta_5^2, \gamma_2 = 1$ | $3x^2+3x+1$ | $(1,2,4,2,1)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5^3,\zeta_5^2,\zeta_5^3)$ | 5 | $\gamma_1 = -\zeta_5^3 - \zeta_5^2 - 1, \gamma_2 = 1$ | $x^2+x+1$ | $(1,3,2,3,1)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5^3,1,\zeta_5^3)$ | 5 | $\gamma_1 = \zeta_5^3 + \zeta_5^2, \gamma_2 = 1$ | $3x^2+3x+2$ | $(2,3,0,3,2)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5^4,1,\zeta_5^4)$ | 5 | $\gamma_1 = -\zeta_5^3 - \zeta_5^2 - 1, \gamma_2 = 1$ | $4x^2+4x+1$ | $(1,4,0,4,1)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5,\zeta_5^2,\zeta_5)$ | 5 | $\gamma_1 = \zeta_5^2 + \zeta_5^3, \gamma_2 = 1$ | $3x^2+3x$ | $(0,1,2,1,0)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5^4,1,\zeta_5^4)$ | 5 | $\gamma_1 = -\zeta_5^2 - \zeta_5^3 - 1, \gamma_2 = 1$ | $4x^2+4x+1$ | $(1,4,0,4,1)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,1,\zeta_5,1)$ | 5 | $\gamma_1 = -\zeta_5^2 - \zeta_5^3 - 1, \gamma_2 = 1$ | $4x^2+4x+2$ | $(2,4,0,4,2)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5,1,\zeta_5)$ | 5 | $\gamma_1 = -\zeta_5^2 - \zeta_5^3 - 1, \gamma_2 = 1$ | $x^2+x+4$ | $(4,1,0,1,4)$ | $(2.23,2.23,2.23,2.23,2.23)$ | ✓ |
| $(0,0,\zeta_5^2,\zeta_5^2,\zeta_5^2)$ | 5 | $\gamma_1 = 2, \gamma_2 = 1$ | $2$ | $(2,2,2,2,2)$ | $(5,0,0,0,0)$ | |
| $(0,0,1,\zeta_7^2,\zeta_7^5,\zeta_7^2,1)$ | 7 | $\gamma_1 = \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2, \gamma_2 = \zeta_7^5 + \zeta_7^2 + 1$ | $4x^2+4x+6$ | $(6,0,2,5,2,0,6)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,1,\zeta_7^3,\zeta_7^4,\zeta_7^3,1)$ | 7 | $\gamma_1 = -\zeta_7^5 - \zeta_7^2 - 1, \gamma_2 = \zeta_7^4 + \zeta_7^3 + 1$ | $6x^2+6x+2$ | $(2,0,3,4,3,0,2)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7,1,\zeta_7^2,1,\zeta_7)$ | 7 | $\gamma_1 = -\zeta_7^4 - \zeta_7^3 - 1, \gamma_2 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2$ | $5x^2+5x+5$ | $(5,1,0,2,0,1,5)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7,\zeta_7^6,\zeta_7^3,\zeta_7^6,\zeta_7)$ | 7 | $\gamma_1 = \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2, \gamma_2 = \zeta_7^5 + \zeta_7^2 + 1$ | $3x^2+3x+2$ | $(2,1,6,3,6,1,2)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^2,\zeta_7^4,1,\zeta_7^4,\zeta_7^2)$ | 7 | $\gamma_1 = \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2, \gamma_2 = \zeta_7^5 + \zeta_7^2 + 1$ | $4x^2+4x+1$ | $(1,2,4,0,4,2,1)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^2,\zeta_7^4,\zeta_7^4,\zeta_7^4,\zeta_7^2)$ | 7 | $\gamma_1 = \zeta_7^5 + \zeta_7^2 + 2, \gamma_2 = \zeta_7^5 + \zeta_7^2 + 1$ | $x^4+2x^3+4x^2+3x+6$ | $(6,2,4,4,4,2,6)$ | $(2.1,3.04,3.04,1.91,1.91,3.04,3.04)$ | |
| $(0,0,\zeta_7^3,\zeta_7^2,\zeta_7^2,\zeta_7^2,\zeta_7^3)$ | 7 | $\gamma_1 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2 + 1, \gamma_2 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2$ | $3x^4+6x^3+5x^2+2x+1$ | $(1,3,2,2,2,3,1)$ | $(5.49,1.35,2.39,1.35,1.35,2.39,1.35)$ | |
| $(0,0,\zeta_7^4,\zeta_7^6,\zeta_7^2,\zeta_7^6,\zeta_7^4)$ | 7 | $\gamma_1 = \zeta_7^5 + \zeta_7^4 + \zeta_7^3 + \zeta_7^2, \gamma_2 = \zeta_7^5 + \zeta_7^2 + 1$ | $4x^2+4x+3$ | $(3,4,6,2,6,4,3)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^4,\zeta_7,1,\zeta_7,\zeta_7^4)$ | 7 | $\gamma_1 = -\zeta_7^5 - \zeta_7^2 - 1, \gamma_2 = \zeta_7^4 + \zeta_7^3 + 1$ | $x^2+x+2$ | $(2,4,1,0,1,4,2)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^5,\zeta_7^2,\zeta_7^2,\zeta_7^2,\zeta_7^5)$ | 7 | $\gamma_1 = \zeta_7^4 + \zeta_7^3 + 2, \gamma_2 = \zeta_7^4 + \zeta_7^3 + 1$ | $2x^4+4x^3+x^2+6x+6$ | $(6,5,2,2,2,5,6)$ | $(0.60,4.31,1.69,1.69,1.69,1.69,4.31)$ | |
| $(0,0,\zeta_7^5,\zeta_7^2,\zeta_7,\zeta_7^2,\zeta_7^5)$ | 7 | $\gamma_1 = -\zeta_7^5 - \zeta_7^2 - 1, \gamma_2 = \zeta_7^4 + \zeta_7^3 + 1$ | $x^2+x+3$ | $(3,5,2,1,2,5,3)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^6,\zeta_7^2,\zeta_7^3,\zeta_7^2,\zeta_7^6)$ | 7 | $\gamma_1 = -\zeta_7^4 - \zeta_7^3 - 1, \gamma_2 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2$ | $6x^2+6x+1$ | $(1,6,2,3,2,6,1)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^3,\zeta_7^4,\zeta_7^2,\zeta_7^4,\zeta_7^3)$ | 7 | $\gamma_1 = \zeta_7^6 + \zeta_7^5 + \zeta_7^2 + \zeta_7, \gamma_2 = \zeta_7^6 + \zeta_7 + 1$ | $2x^2+2x+6$ | $(6,3,4,2,4,3,6)$ | $(2.64,2.64,2.64,2.64,2.64,2.64,2.64)$ | ✓ |
| $(0,0,\zeta_7^6,1,1,1,\zeta_7^6)$ | 7 | $\gamma_1 = \zeta_7^6, \gamma_2 = -\zeta_7^5 - \zeta_7^4 - \zeta_7^3$ | $4x^4+x^3+2x^2+5x+1$ | $(1,6,0,0,0,6,1)$ | $(5.49,1.35,2.39,1.35,1.35,2.39,1.35)$ | |
| $(0,0,\zeta_{11}^{10},\ldots,\zeta_{11}^{10})$ | 11 | $\gamma_1 = 8, \gamma_2 = 7$ | $10$ | $(10,10,...,10)$ | $(11,0,0,...,0)$ | |

get $f = 3x^2 + 3x$, and so $f(0) = f(4) = 0$. Thus the truth-table is $(0,1,2,1,0)$, the Walsh spectrum is $(\sqrt{5}, \sqrt{5}, \sqrt{5}, \sqrt{5}, \sqrt{5})$. Therefore the spectrum is flat, it means that this function is a generalized bent function. The matrix $C$ obtained from $\underline{a}$ is given below, which is the same matrix illustrated in Example 2.

$$C = \begin{bmatrix} 0^{f(0-0)} & 0^{f(0-1)} & \zeta_p^{f(0-2)} & \zeta_p^{f(0-3)} & \zeta_p^{f(0-4)} \\ \zeta_p^{f(1)} & 0^{f(0)} & 0^{f(4)} & \zeta_p^{f(3)} & \zeta_p^{f(2)} \\ \zeta_p^{f(2)} & \zeta_p^{f(1)} & 0^{f(0)} & 0^{f(4)} & \zeta_p^{f(3)} \\ \zeta_p^{f(3)} & \zeta_p^{f(2)} & \zeta_p^{f(1)} & 0^{f(0)} & 0^{f(4)} \\ 0^{f(4)} & \zeta_p^{f(3)} & \zeta_p^{f(2)} & \zeta_p^{f(1)} & 0^{f(0)} \end{bmatrix}$$

We did an exhaustive search for almost $p$-ary sequences of type $(\gamma_1, \gamma_2)$ and period $n+2$ with two consecutive zero-symbols for $p \in \{5, 7, 11\}$. We tabulate our results in Table 1. The Boolean function $f$ obtained from the corresponding sequence, its truth-table, Walsh spectrum and bentness are given in this table. It is seen that we generally obtain a bent function from a NPS. Moreover, we obtain some other functions with 3 distinct Walsh coefficients. These functions come from the same class of sequences, namely almost $p$-ary NPS with two distinct autocorrelation coefficients, but they are not bent.

## 5. CDMA Simulation

In this section, we explain how sequences are used in CDMA. First, we examine the CDMA structure (see Figure 1). At the transmitter side, we first choose data from set $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, and convert the data to complex data obtained by taking corresponding power of $\zeta_p$. For example, when $p = 3$ and the data is $(0,1,2,1,1)$, the complex data is $(\zeta_3^0, \zeta_3^1, \zeta_3^2, \zeta_3^1, \zeta_3^1)$. In the next step of CDMA, each term of the complex data is multiplied by the sequence given to the user and then the spread message is obtained, the spread messages of each user are added to each other to obtain the transmitted message. In the Rayleigh channel the signal

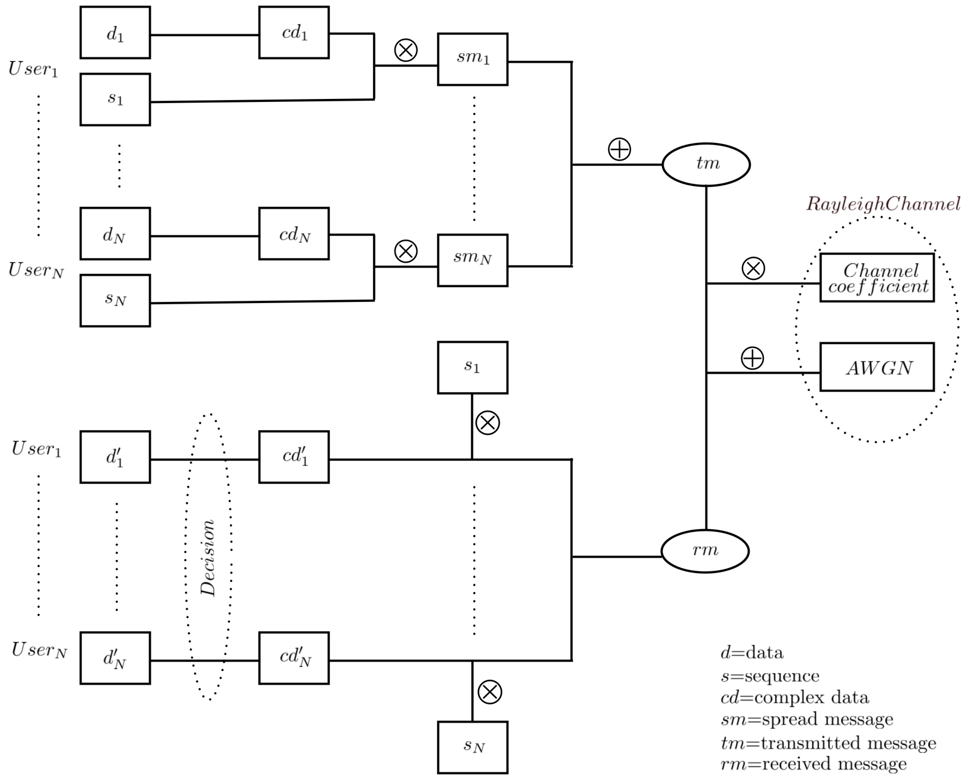

Fig. 1. Structure of CDMA

is multiplied by the channel coefficient and AWGN is added. So, the received message is obtained. At the receiver side, the received message is multiplied by the user's sequence and $cd'$ is obtained. In the decision process, for each component of $cd'$, the element closest to any of the set $\mathcal{E}_p$ is chosen as the corresponding component of the $d'$. We give an example below.

*Example 4:* Let $\mathcal{E}_3 = \{1, \zeta_3, \zeta_3^2\} \approx \{1, -0.49 + 0.86j, -0.5 - 0.86j\}$ and $cd' = \{-2.5 - 0.81j, -1.3 - 0.69j\}$. Now, we take the difference between $(-2.5 - 0.81j)$ and each element in $A$, and calculate their norms.

$$\begin{aligned}\{|-2.5-0.8j-A_i|\}_{i=1,2,3} &= \{|3.5+0.81j)|, |2.01+1.67j|,\\ &\quad |2-0.05j|\}\\ &= \{\sqrt{3.5^2+0.81^2}, \sqrt{2.01^2+1.67^2},\\ &\quad \sqrt{2^2+(-0.05)^2}\}\\ &\approx \{3.6, 2.61, 2\}\end{aligned}$$

The minimum value is 2, obtained by the $(-0.5 - 0.86j) \approx \zeta_3^2 \in A$. Hence, $d' = 2$ for $cd' = (-2.5 - 0.81j)$. Similarly, the $d'$ for $cd' = (1.3 - 0.69j)$ is 0. Therefore, $cd' = \{-2.5 - 0.81j, -1.3 - 0.69j\}$ is easily converted to $d' = \{2, 0\}$.

We simulated Figure 1 by using nearly perfect sequences $a_1 = (0, 0, \zeta_3^2, 1, \zeta_3^2, \ldots)$ of type $(-1, 1)$, $a_2 = (0, 0, \zeta_3^2, 1, \zeta_3^2, \zeta_3^2, \zeta_3^2, \zeta_3, \zeta_3^2, \zeta_3^2, \zeta_3^2, 1, \zeta_3^2, \ldots)$ of type $(1, 3)$, $a_3 = (0, 0, 1, \zeta_2, 1, \ldots)$ of type $(-2, 1)$ and $a_4 = (0, 0, 1, 1, 1, \zeta_2, \zeta_2, \zeta_2, 1, \zeta_2, \zeta_2, 1, \zeta_2, \ldots)$ of type $(0, -1)$. We selected the number of users as 2, 3 and 4 in the simulations. We have simulated by using Python program language where the data length fixed to $10000$ and each simulation repeated 11 times. The simulation results are given in Figures 2, 3, 4, 5. In the figures, we compare the bit-error-rate (BER) performance of each sequence, where BER is defined to be the ratio of the number of errors to the number of bits. It is seen that the larger period of sequence is chosen, the better BER performance is obtained when $p$ and the number of users are fixed (see Figures 2 and 3 or Figures 4 and 5). On the other hand, the smaller $p$ is chosen, the better BER is obtained when the period of sequence and the number of users are fixed (see Figures 2 and 4 or Figures 3 and 5). The BER performance is dependent on the number of users for any fixed sequence. It is seen that an increase in the number of users proportionally decreases the BER performance. We see the best simulation results is obtained by using $a_4$ (see Figure 5). Note that the increase in the number of users for this sequence affects the BER performance very little. As a result, for a multi-user case, if $p$ is small, choose the period of sequence as large as possible, so that the better BER performance is obtained.

In [12, Section 5.5], the BER performance of CDMA with $M$-sequence and orthogonal Gold sequence in AWGN or Rayleigh channel is given. In both channels, orthogonal Gold sequences have better results. The BER performance in our simulation is not as good as in [12, Section 5.5] because we used almost $p$-ary NPS of type $(\gamma_1, \gamma_2)$. However, for the $a_4$ sequence we get approximately the same BER performance as in [12, Section 5.5, Fig.5.20]. For instance, in [12, Section 5.5, Fig.5.20], for $dB = 8$, $BER \approx 0.05$ where the number of users is 7. In Figure 5, for $dB = 8$, $BER \approx 0.05$ where the number of users is 4. It would be a good future work to device an efficient method for recovering the received message.

## 6. Conclusion

The main objective of this study is the application of almost $p$-ary sequences to obtain cryptographic bent functions and BER analysis on CDMA. By using a modification of well-known conversion between sequences and boolean functions, we generally obtained generalized bent function from an almost $p$-ary NPS except for some classes of sequences. On the other hand, we simulated BER analysis on CDMA by devising some almost $p$-ary NPS. According to these simulations, these sequences are not perfectly proper for the CDMA, but we consider that with a few adjustments, better results can be obtained.

## Acknowledgments

The authors are supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Project No: 116R026.

## References

[1] P. V. Kumar, R. A. Scholtz, and L. R. Welch. ”Generalized bent functions and their properties.” Journal of Combinatorial Theory, Series A 40.1 (1985): 90-107.

[2] S. Kurt, and O. Yayla. ”Near Butson-Hadamard Matrices and Nonlinear Boolean Functions.” International Conference on Number-Theoretic Methods in Cryptology. Springer, Cham, 2017.

[3] B. Özden, and O. Yayla. ”Almost p-ary Sequences.” arXiv preprint arXiv:1807.11412 (2018).

[4] D. Jungnickel, and A. Pott. Perfect and Almost Perfect Sequences. Discrete Applied Mathematics 95 (1999): 331-359.

[5] K.-U Schmidt. Quaternary Constant-Amplitude Codes for Multicode CDMA. IEEE Transactions on Information Theory 55 (2007): 1824-1832.

[6] C.-L I, and R. D. Gitlin, Multi-code CDMA wireless personal communications networks, Proc. IEEE ICC’95, Vol. 2, pp10601064, June 1995.

[7] J. Hollon, M. Rangaswamy, and P. Setlur. ”New families of optimal high-energy ternary sequences having good correlation properties.” Journal of Algebraic Combinatorics (2018): 1-38.

[8] S. W. Golomb, and G. Gong. Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University Press, 2005.

[9] T. Helleseth, and P. V. Kumar, Sequences with low correlation, in: Vera S. Pless and W. Cary Huffman, eds., Handbook in Coding Theory, volume II, chapter 21, pp. 1765-1853, Elsevier Science B.V., Amsterdam, 1998.

[10] H. Y. Liu, and K. Q. Feng. ”New results on nonexistence of perfect p-ary sequences and almost p-ary sequences.” Acta Mathematica Sinica, English Series 32.1 (2016): 2-10.

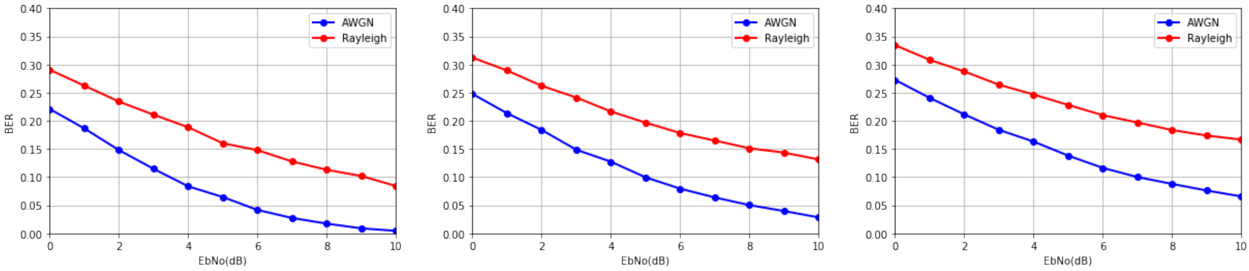

Fig. 2. BER performance of CDMA with $a_1$ and 2, 3, 4 users respectively

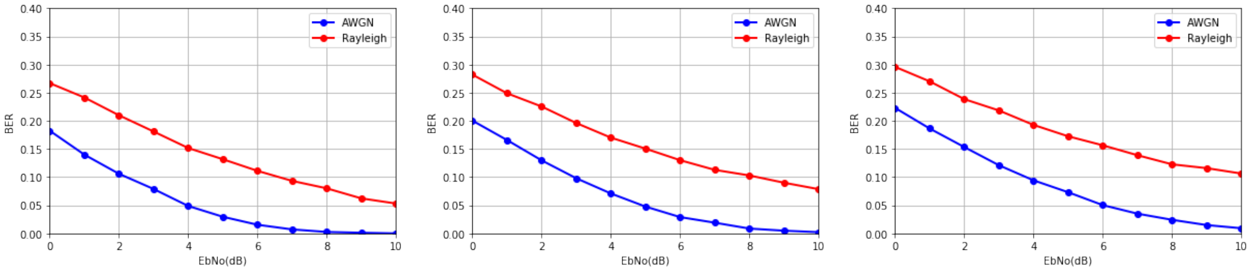

Fig. 3. BER performance of CDMA with $a_2$ and 2, 3, 4 users respectively

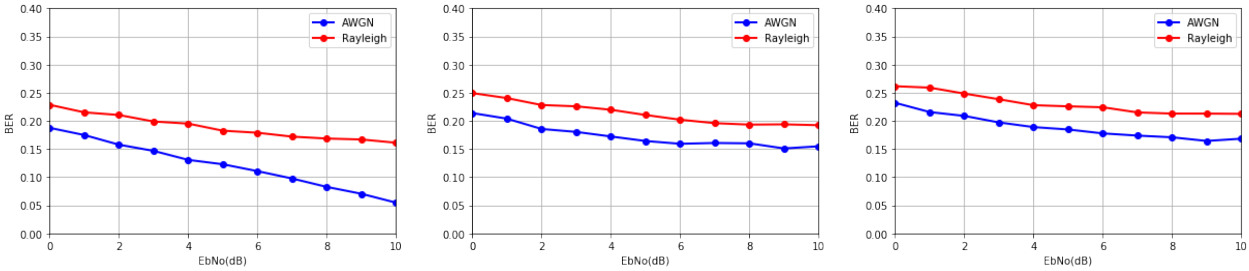

Fig. 4. BER performance of CDMA with $a_3$ and 2, 3, 4 users respectively

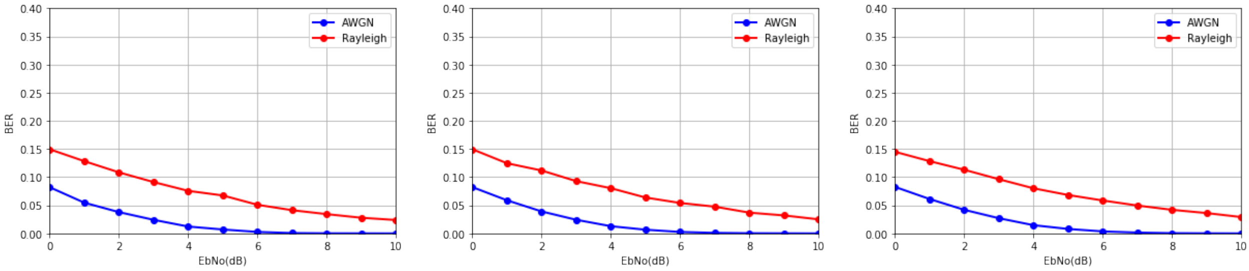

Fig. 5. BER performance of CDMA with $a_4$ and 2, 3, 4 users respectively

[11] Y. M. Chee, Y. Tan, and Y. Zhou. ”Almost p-ary perfect sequences.” International Conference on Sequences and Their Applications. Springer, Berlin, Heidelberg, 2010.

[12] H. Harada, and R. Prasad. Simulation and software radio for mobile communications. Vol. 1. Artech House, 2002.