Spectral and Nonlinear Properties of the Complete Quaternary Code

Nadiia Kazakova[1][0000-0003-3968-4094] and Artem Sokolov[2][0000-0003-0283-7229]

[1] Odesa State Environmental University, Ukraine
[2] Odesa National Polytechnic University, Ukraine
kaz2003@ukr.net

Abstract. The current stage of development of information technologies is characterized by the active introduction of the functions of many-valued logic. In particular, many-valued logic functions are used in cryptography to build high-quality cryptographic primitives with a high level of nonlinearity. This circumstance determines the need for more detailed research of the nonlinearity of the complete codes of functions of many-valued logic. Because of the possibility of representing constructions of almost all modern ciphers by 4-functions, they occupy a special place among other q values in the research of the level of nonlinearity. This paper presents a universal method for calculating the possible absolute values of the Vilenkin-Chrestenson transform coefficients of many-valued logic functions. This method is applied to 4-functions of length $N = 4$ and $N = 16$. As a result, 5 spectral classes of vectors of length $N = 4$, and 36 spectral classes of vectors of length $N = 16$ were discovered, each of which has a unique elementary structure, and, accordingly, the certain value of nonlinearity. Because of the dependence of such a fundamental concept of MC-CDMA technology as the Peak-to-Average Power Ratio of the applied signals and their spectral properties, the results obtained can also be used to calculate the maximum cardinality values of constant amplitude codes constructed based on many-valued logic functions.

Keywords: Many-Valued Logic Function, Cryptography, Nonlinearity, PAPR.

1 Introduction and Statement of the Problem

The current stage in the development of cryptography is characterized by the great attention of researchers to the methods of many-valued logic [1]. Methods of many-valued logic are used both to increase the security of quantum cryptographic algorithms [2, 3] as well as to create new cryptographic primitives [4, 5], and traditional cryptographic algorithms [6], characterized by increased security [7]. There are also methods to estimate the cryptographic quality of existing cryptographic algorithms represented by the functions of many-valued logic. To estimate the cryptographic quality of many-valued logic functions, a set of criteria [2] has been introduced, among which the most important is the criterion of nonlinearity.

This circumstance makes it especially important to research the nonlinear properties of many-valued logic functions, which, due to the interconnection between nonlinearity and the spectral properties of many-valued logic functions, is closely related to the issue of spectral classification of complete quaternary code.

On the other hand, there is a direct relationship between the spectral properties of sequences and such a parameter as the Peak-to-Average Power Ratio (PAPR) of their spectrum, which plays a significant role in the case of their application in MC-CDMA technology [8]. That is, the problem of spectral classification of the complete code of quaternary sequences is also equivalent to the problem of determining the maximum cardinalities of actively used quaternary C-codes [9], which have a given level of the PAPR of the Vilenkin-Chrestenson spectrum.

At the moment, in the literature the spectral classification of the complete codes of ternary sequences of lengths $N = 3$ and $N = 9$ is already performed [10], nevertheless, the spectral properties of quaternary sequences remain unknown.

The purpose of this paper is to develop a method for the spectral classification of quaternary sequences, as well as to carry out the spectral classification of the full set of quaternary sequences of lengths $N = 4$ and $N = 16$.

2 Basic Definitions

Let's introduce the basic definitions. As an alphabet of sequences of 4-valued logic, it is convenient to consider the set of fourth roots of unity

$$z_k = e^{j\frac{2\pi}{4}k}, \quad k \in \{0,1,2,3\}, \tag{1}$$

then the alphabet of the considered in this paper vectors will consist of the following values

$$z_0 = e^{j\frac{2\pi}{4}0} = 1; \quad z_1 = e^{j\frac{2\pi}{4}1} = j; \quad z_2 = e^{j\frac{2\pi}{4}2} = -1; \quad z_2 = e^{j\frac{2\pi}{4}3} = -j. \tag{2}$$

For each sequence of 4-logic, we define the vector of the Vilenkin-Chrestenson transform [11] as the product of some sequence A of 4-valued logic by the transposed Vilenkin-Chrestenson matrix

$$\Omega_f = f \cdot V^T, \tag{3}$$

where the Vilenkin-Chrestenson matrix is defined by the following recurrent construction [4]

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \quad V_4 = \begin{bmatrix} z_0 & z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 & z_3 \\ z_0 & z_2 & z_0 & z_2 \\ z_0 & z_3 & z_2 & z_1 \end{bmatrix}. \tag{4}$$

In expression (4) matrices V are represented in symbolic form, i.e. the summation is performed relative to the indices z_i.

The quaternary sequence of length $N = 4^k$ can be considered as the truth table of the many-valued logic function of k variables, which are used to estimate the quality of cryptographic algorithms as well as for the construction of perspective cryptographic primitives [4].

Today there is a known method for estimating the nonlinearity of many-valued logic functions [12] using the coefficients of the Vilenkin-Chrestenson transform

$$N_f = \begin{cases} q^k - \max\left\{\left|\Omega_f\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W_f\right|\right\}, & q = 2, \end{cases} \tag{5}$$

where W_f are the Walsh-Hadamard transform coefficients which are used instead of Vilenkin-Chrestenson transform coefficients in the case of Boolean functions [13].

The formula (5) for calculating the nonlinearity of the many-valued logic functions is basic in cryptography and is used to estimate the level of confusion that can be provided by one or another many-valued logic functions used in cryptographic algorithms.

The formula (5) also shows a direct relationship between nonlinearity and spectral properties of many-valued logic sequences. Thus, more detailed research of the structure of the Vilenkin-Chrestenson spectrum of functions of many-valued logic will allow a better understanding of the possible values of their nonlinearity, as well as discovering the sets of sequences with a given level of nonlinearity.

Note also that from the spectral properties of many-valued logic sequences follows such an important characteristic as the PAPR, which is decisive for their use as C-codes in MC-CDMA technology [7]

$$\kappa = \frac{P_{\max}}{P_{cp}} = \frac{1}{N}\max_t\left\{\left|\Omega_f\right|^2\right\} \tag{6}$$

where $P_{\max}$ is the peak power of the signal Ω_f,

P_{av} is the average power of the signal Ω_f,

N is the length of the sequence.

So, such practically valuable properties of sequences of many-valued logic as nonlinearity and PAPR are the special cases of their spectral properties. This fact makes the task of spectral classification of the sequences of many-valued logic very important.

3 Spectral Classification of Quaternary Sequences of Length $N = 4$

Each quaternary sequence of length $N = 4$ can be represented in the following generalized form

$$A = \{a_1 \quad a_2 \quad a_3 \quad a_4\}, \quad a_i = z_k = e^{j\frac{2\pi}{4}k}, \quad k \in \{0,1,2,3\}. \tag{7}$$

For each such quaternary vector, the Vilenkin-Chrestenson transform can be found by multiplying it by the matrix complex conjugation of the Vilenkin-Chrestenson matrix $S = A \cdot \overline{V_4}$. In this case, in general form, the vector of the Vilenkin-Chrestenson transform coefficients can be represented as follows

$$S = \{s_1 \quad s_2 \quad s_3\}, \; s_i \in \square \; . \tag{8}$$

Each vector A uniquely corresponds to its vector S. The converse is not true, i. e. not for every vector S, $s_i \in \square$, there is such corresponding vector with such coordinates $a_i \in \{1, z_1, z_2, z_3\}$ that equality $S = A \cdot \overline{V_4}$ is valid.

In the general case, the problem of finding nonlinear sequences is the problem of finding sequences with given spectral properties, which implies research of the admissible structures of vectors S, as well as values of their elements for which exists the corresponding vectors in the time domain. This problem is a problem of spectral classification of quaternary vectors of length *N*.

We will perform the spectral classification by the approach [14], i.e. based on the definition of sets of absolute values of spectral vectors.

Let us find out what values the elements s_i can take in the example of the first Vilenkin-Chrestenson transform coefficient s_1. This coefficient is the result of the product of the sequence A in the time domain by the first column of the Vilenkin-Chrestenson matrix. The elements of the sequence A belong to the alphabet $\{z_0, z_1, z_2, z_3\}$, which can be represented in the algebraic form of representing a complex number (2).

Let us denote by K_0, K_1, K_2, K_3 the number of elements z_0, z_1, z_2 and z_3 in the sequence A, respectively. Then the coefficient s_1 will take the values

$$s_1 = [K_0 - K_2] + j[K_1 - K_3], \tag{9}$$

where

$$\begin{cases} K_0 + K_1 + K_2 + K_3 = 4, \\ K_0, K_1, K_2, K_3 \in \{0,1,2,3,4\}. \end{cases} \tag{10}$$

It is easy to find that there are only 35 sets of numbers K_0, K_1, K_2, K_3 that satisfy condition (10)

$$\left[\begin{array}{cccc|cccc|cccc}
K_0 & K_1 & K_2 & K_3 & K_0 & K_1 & K_2 & K_3 & K_0 & K_1 & K_2 & K_3 \\
0 & 0 & 0 & 4 & 0 & 3 & 0 & 1 & 1 & 3 & 0 & 0 \\
0 & 0 & 1 & 3 & 0 & 3 & 1 & 0 & 2 & 0 & 0 & 2 \\
0 & 0 & 2 & 2 & 0 & 4 & 0 & 0 & 2 & 0 & 1 & 1 \\
0 & 0 & 3 & 1 & 1 & 0 & 0 & 3 & 2 & 0 & 2 & 0 \\
0 & 0 & 4 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\
0 & 1 & 0 & 3 & 1 & 0 & 2 & 1 & 2 & 1 & 1 & 0 \\
0 & 1 & 1 & 2 & 1 & 0 & 3 & 0 & 2 & 2 & 0 & 0 \\
0 & 1 & 2 & 1 & 1 & 1 & 0 & 2 & 3 & 0 & 0 & 1 \\
0 & 1 & 3 & 0 & 1 & 1 & 1 & 1 & 3 & 0 & 1 & 0 \\
0 & 2 & 0 & 2 & 1 & 1 & 2 & 0 & 3 & 1 & 0 & 0 \\
0 & 2 & 1 & 1 & 1 & 2 & 0 & 1 & 4 & 0 & 0 & 0 \\
0 & 2 & 2 & 0 & 1 & 2 & 1 & 0 & & & &
\end{array}\right]. \qquad (11)$$

To find the possible absolute values of the coefficient s_1, we substitute solutions (11) into (9), after which, finding the absolute values of complex numbers, we obtain

$$|s_1| = \sqrt{(K_0 - K_2)^2 + (K_1 - K_3)^2} \in \{0, \sqrt{2}, 2, \sqrt{8}, \sqrt{10}, 4\}. \qquad (12)$$

Proposition 1. The set of values (12), and only them, are possible absolute values of the Vilenkin-Chrestenson transform coefficients of vectors of length $N = 4$.

Let us express the value of the first Vilenkin-Chrestenson transform coefficient in terms of the elements of the original sequence

$$\begin{aligned} s_1 &= [a_1 \quad a_2 \quad a_3 \quad a_4] \cdot [z_0 \quad z_0 \quad z_0 \quad z_0]^T = \\ &= [a_1 \quad a_2 \quad a_3 \quad a_4] \cdot [1 \quad 1 \quad 1 \quad 1]^T = \\ &= a_1 + a_2 + a_3 + a_4, \quad a_i \in \{z_0, z_1, z_2, z_3\}. \end{aligned} \qquad (13)$$

Similarly, consider the i^{th} Vilenkin-Chrestenson transform coefficient

$$\begin{aligned} s_i &= [a_1 \quad a_2 \quad a_3 \quad a_4] \cdot [v_0 \quad v_1 \quad v_2 \quad v_3]^T = \\ &= \left[e^{j\beta_1} \quad e^{j\beta_2} \quad e^{j\beta_3} \quad e^{j\beta_4} \right] \cdot \left[e^{j\gamma_1} \quad e^{j\gamma_2} \quad e^{j\gamma_3} \quad e^{j\gamma_4} \right]^T = \\ &= \left[e^{j(\beta_1+\gamma_1)} \quad e^{j(\beta_2+\gamma_2)} \quad e^{j(\beta_3+\gamma_3)} \quad e^{j(\beta_4+\gamma_4)} \right]. \end{aligned} \qquad (14)$$

Since $\beta_i, \gamma_i \in \{z_0, z_1, z_2, z_4\}$ for each s_i, there is a sequence $A' = [a'_1 \quad a'_2 \quad a'_3 \quad a'_4]$, the Vilenkin-Chrestenson transform of which has a coefficient s_1 equal to the given s_i.

Due to Parseval's equality, the minimum value of the Vilenkin-Chrestenson transform coefficient cannot be lower than $q^{k/2} = 4^{\frac{1}{2}} = 2$. So, the values of the Vilenkin-Chrestenson transform coefficients of quaternary sequences $|s_i| = 0$ and $|s_i| = \sqrt{2}$ cannot be the maximum absolute values in the Vilenkin-Chrestenson transform vector. Thus, the set of possible values of nonlinearity by (5) is

$$N_f \in 4 - \{4, \sqrt{10}, \sqrt{8}, 2\} = \{0, 0.8377, 1.1716, 2\}. \qquad (15)$$

We can highlight the method for calculating the possible absolute values of the Vilenkin-Chrestenson transform coefficients, and, accordingly, the possible values of nonlinearity and PAPR, in the form of specific steps:

Step 1. Present in general form the absolute value of the first Vilenkin-Chrestenson transform coefficient s_1 in terms of the numbers $K_0, K_1, ..., K_{q-1}$ of elements of the many-valued logic sequence alphabet.

Step 2. Find possible values $K_0, K_1, ..., K_{q-1}$ that satisfy the condition

$$\begin{cases} K_0 + K_1 + ... + K_{q-1} = N, \\ K_0, K_1, ..., K_{q-1} \in \{0,1,..,N\}. \end{cases} \quad (16)$$

Step 3. Substitute the possible values $K_0, K_1, ..., K_{q-1}$ into the expression obtained in Step 1 for the absolute value of the first Vilenkin-Chrestenson transform coefficient s_1 in terms of the numbers $K_0, K_1, ..., K_{q-1}$ of the many-valued logic sequence alphabet. In this case, because of Statement 1, the resulting set of values will constitute the full set of possible values of all the coefficients of the Vilenkin-Chrestenson transform.

Step 4. Calculate the possible values of nonlinearity and PAPR by formulas (5) and (6) for the complete set of possible values of all Vilenkin-Chrestenson transform coefficients obtained at Step 3.

The results of calculations showed that for vectors of length $N = 4$ there are five spectral classes of vectors (Table 1), for each of which the cardinality of the class, the value of nonlinearity and PAPR as well as the representative sequence are provided.

Table 1. Spectral classification of quaternary vectors of length $N = 4$

No.	Spectral class represented in the form of irrationalities	Class cardinality	Nonlinearity	PAPR	Representative sequence
1	$\{4(1), 0(3)\}$	16	0	4.0	0000
2	$\{\sqrt{10}(1), \sqrt{2}(3)\}$	128	0.8377	2.5	0001
3	$\{\sqrt{8}(1), 2(2), 0(1)\}$	64	1.1716	2.0	0011
4	$\{\sqrt{8}(2), 0(2)\}$	16	1.1716	2.0	0022
5	$\{2(4)\}$	32	2.0000	1.0	0002

Analysis of the data presented in Table 1 shows that the complete code of quaternary sequences of length $N = 4$ can be classified into five spectral classes, among which there is a class of affine functions [15] of cardinality $J_1 = 16$, as well as the class of bent-functions [16] of cardinality $J_5 = 32$.

In Fig. 1, a histogram of the distribution of nonlinearity of quaternary sequences of length $N = 4$ is shown.

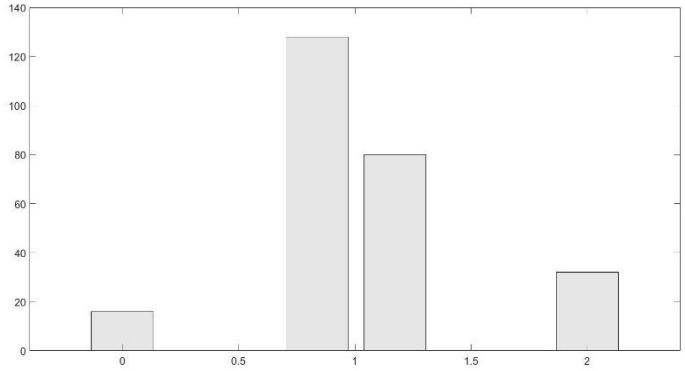

Fig. 1. Histogram of nonlinearity distribution of quaternary sequences of length $N = 4$.

4 Spectral Classification of Quaternary Sequences of Length $N = 16$

It should be noted that sequence length $N = 16$ is very important in modern cryptographic applications. So, the problem of spectral classification of the complete set of quaternary sequences of length $N = 16$ is of special interest in the terms of their usage in cryptography.

Expression (16) for the case of quaternary sequences of length $N = 16$ takes the following form

$$\begin{cases} K_0 + K_1 + K_2 + K_3 = 16, \\ K_0, K_1, K_2, K_3 \in \{0,1,2,3,...,16\}, \end{cases} \tag{17}$$

while the total number of sets of numbers K_0, K_1, K_2, K_3 that satisfy condition (17) is 969.

Based on the set of suitable K_0, K_1, K_2, K_3 sets, and taking into account Statement 1, as well as the formula for the absolute value of a complex number, we can write down the set of possible absolute values of the Vilenkin-Chrestenson transform coefficients of quaternary sequences of length $N = 16$

$$\begin{gathered} |s_i| \in \{0, \sqrt{2}, 2, \sqrt{8}, \sqrt{10}, 4, \sqrt{18}, \sqrt{20}, \sqrt{26}, \sqrt{32}, \\ \sqrt{34}, 6, \sqrt{40}, \sqrt{50}, \sqrt{52}, \sqrt{58}, 8, \sqrt{68}, \sqrt{72}, \sqrt{74}, \\ \sqrt{80}, \sqrt{82}, \sqrt{90}, \sqrt{98}, 10, \sqrt{104}, \sqrt{106}, \sqrt{116}, \\ \sqrt{122}, \sqrt{128}, \sqrt{130}, \sqrt{136}, 12, \sqrt{146}, \sqrt{148}, \\ \sqrt{160}, \sqrt{170}, \sqrt{178}, 14, \sqrt{200}, \sqrt{226}, 16\}. \end{gathered} \tag{18}$$

In the case of quaternary sequences of length $N = 16$, due to Parseval's equality, the minimum value of the coefficient of the Vilenkin-Chrestenson transform cannot be less

than $q^{k/2} = 4^{\frac{2}{2}} = 4$. The values of the Vilenkin-Chrestenson transform coefficients $|s_i| = 0, \sqrt{2}, 2, \sqrt{8}, \sqrt{10}$ of quaternary sequences cannot be maximum in the Vilenkin-Chrestenson transform to vector. The full class of possible values of the nonlinearity of quaternary sequences of length $N = 16$ by the formula (5) is

$$\begin{aligned} N_f \in \{&252, 251.76, 251.53, 250.90, 250.34, 250.17, 250,\\ &249.68, 248.93, 248.79, 248.38, 248, 247.75, 247.51,\\ &247.40, 247.06, 246.94, 246.51, 246.10, 246.00,\\ &245.80, 245.70, 245.23, 244.95, 244.69, 244.60,\\ &244.34, 244.00, 243.92, 243.83, 243.35, 242.96,\\ &242.66, 242, 241.86, 240.97, 240\}. \end{aligned} \tag{19}$$

We present Table 2, which represents the number of quaternary sequences of length $N = 16$ having a given maximum absolute value of the Vilenkin-Chrestenson transform coefficients and, accordingly, the given value of nonlinearity and PAPR.

Table 2. Spectral classification of quaternary vectors of length $N = 16$

No.	Value	Nonlinearity	Cardinality of the class	PAPR	Representative sequence
1	16	0	64	16.00	0000000000000000
2	$\sqrt{226}$	0.97	2048	14.13	0000000000000001
3	$\sqrt{200}$	1.86	15360	12.50	0000000000000011
4	14	2.00	16384	12.25	0000000000000002
5	$\sqrt{178}$	2.66	71680	11.13	0000000000000111
6	$\sqrt{170}$	2.96	245760	10.63	0000000000000012
7	$\sqrt{160}$	3.35	232960	10.00	0000000000001111
8	$\sqrt{148}$	3.83	1146880	9.25	0000000000000112
9	$\sqrt{146}$	3.92	559104	9.13	0000000000011111
10	12	4.00	921600	9.00	0000000000000022
11	$\sqrt{136}$	4.34	1025024	8.50	0000000000111111
12	$\sqrt{130}$	4.60	5191680	8.13	0000000000001112

Table 3. Spectral classification of quaternary vectors of length $N = 16$ (continuation)

No.	Value	Nonlinearity	Cardinality of the class	PAPR	Representative sequence
13	$\sqrt{128}$	4.69	823488	8.00	0000000011111111
14	$\sqrt{122}$	4.95	8601600	7.63	0000000000000122
15	$\sqrt{116}$	5.23	8945664	7.25	0000000000011112
16	$\sqrt{106}$	5.70	16400384	6.63	0000000000111112
17	$\sqrt{104}$	5.80	27955200	6.50	0000000000001122
18	10	6.00	43450368	6.25	0000000000000222
19	$\sqrt{98}$	6.10	13172736	6.13	0000000001113333
20	$\sqrt{90}$	6.51	67092480	5.63	0000000000011122
21	$\sqrt{82}$	6.94	130433024	5.13	0000000000001222
22	$\sqrt{80}$	7.06	122179584	5.00	0000000000111122
23	$\sqrt{74}$	7.40	172720128	4.63	0000000000122233
24	$\sqrt{72}$	7.51	95625216	4.50	0000000000122333
25	$\sqrt{68}$	7.75	300613632	4.25	0000000000011222
26	8	8.00	195660800	4.00	0000000000002222
27	$\sqrt{58}$	8.38	510885888	3.63	0000000000021222
28	$\sqrt{52}$	8.79	586743808	3.25	0000000000220222
29	$\sqrt{50}$	8.93	885211136	3.13	0000000000220122
30	$\sqrt{40}$	9.68	628068352	2.50	0000000100021222
31	6	10.00	109428736	2.25	0000000200020222
32	$\sqrt{34}$	10.17	324706304	2.13	0000000200120222
33	$\sqrt{32}$	10.34	22414592	2.00	0000000200220222
34	$\sqrt{26}$	10.90	12189696	1.63	0000001200222310
35	$\sqrt{20}$	11.53	2015232	1.25	0000001201323211
36	4	12.00	200704	1.00	0000002202020220

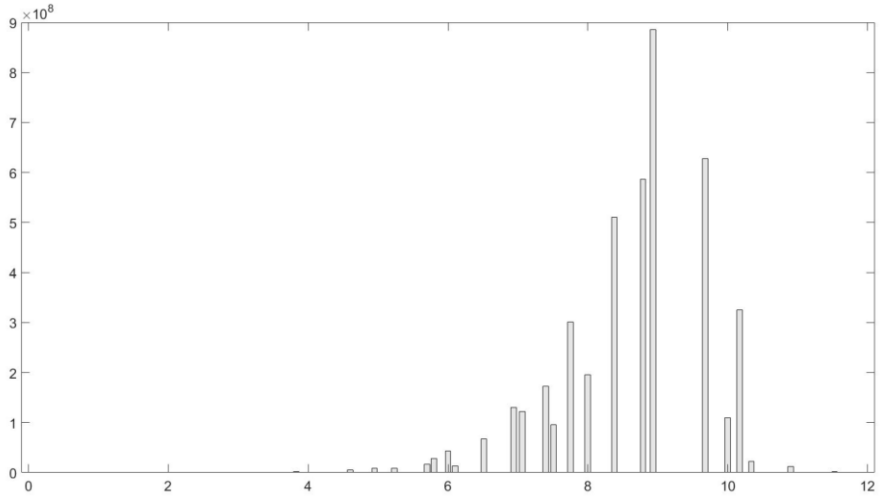

Fig. 2. Histogram of nonlinearity distribution of quaternary sequences of length $N = 16$.

The performed spectral classification of quaternary sequences of length $N = 16$ is a theoretical basis for the synthesis of sets of 4-functions with a given level of nonlinearity. These sets are the initial material for the construction of cryptographically strong generators of pseudo-random key sequences, as well as cryptographic primitives of block symmetric ciphers and hash functions. Table 2 and Fig. 2 also specifies the maximum cardinalities of the C-code classes for MC-CDMA technology.

5 Conclusion

In conclusion, we note the main results of the research:

1. A method for calculating the possible values of the Vilenkin-Chrestenson transform coefficients is proposed. Because of the dependence of the spectral properties of the sequences and the determination of nonlinearity and PAPR, the proposed method can be applied to estimate the possible values of nonlinearity and PAPR of sequences of many-valued logic. The proposed method is suitable for arbitrary values of q and N, however, in this work, it was applied for the case of quaternary sequences of lengths $N = 4$ and $N = 16$.

2. A spectral classification of the full quaternary code of the lengths $N = 4$ and $N = 16$ was performed, as a result of which 5 spectral classes of sequences of length $N = 4$ was distinguished as well as 36 spectral classes of sequences of length $N = 16$, each of which has a unique elementary structure, and, accordingly, a value of nonlinearity and PAPR.

3. The resulting spectral classification is a theoretical basis for constructing sets of many-valued logic functions with a given level of nonlinearity used in cryptography, as well as for constructing C-codes used to reduce the PAPR in MC-CDMA technology.

References

1. Sokolov, A. V., Zhdanov, O. N.: Prospects for the application of many-valued logic functions in cryptography. Int. Conf. Theory Appl. Fuzzy Sys. Soft Comput.: 331–339 (2018). https://doi.org/10.1007/978-3-319-91008-6_33
2. Gnatyuk, S., Zhmurko, T., Falat, P.: Efficiency increasing method for quantum secure direct communication protocols. IEEE Proc. 8th Int. Conf. Intell. Data Acquis. Adv. Comput. Sys.: Technol. Appl. (IDAACS): 468–472 (2015). https://doi.org/10.1109/IDAACS.2015.7340780
3. Gnatyuk, S. O., Zhmurko, T. O., Kinzeryavy, V. M., Siyilova, N. A.: Method for quality evaluation of trit pseudorandom sequence to cryptographic applications. Inf. Technol. Secur. **2**(3): 108–116 (2015). https://doi.org/10.20535/2411-1031.2015.3.2.60891
4. Sokolov, A. V., Zhdanov, O. N.: Cryptographic Constructions Based on Many-Valued Logic Functions. Scientific Thought (2020). https://doi.org/10.12737/1045434
5. Bessalov, A. V.: Calculation of parameters of cryptographically robust "Edwards curve" over the fields of characteristics 5 and 7. Cybersecur. Educ. Sci. Tech. **1**(1): 94–104 (2018). https://doi.org/10.28925/2663-4023.2018.1.94104
6. Zhdanov, O. N., Sokolov, A. V.: Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. Far East J. Electron. Commun. **16**(3): 573–589 (2015). https://doi.org/10.17654/ec016030573
7. Bessalov, A., Grubiyan, E., Sokolov, V., Skladannyi, P.: 3- and 5-isogenies of supersingular Edwards curves. Cybersecur. Educ. Sci. Tech. **4**(8): 6–21 (2020). https://doi.org/10.28925/2663-4023.2020.8.621
8. Paterson, K. G.: Sequences for OFDM and multi-code CDMA: Two problems in algebraic coding theory, sequences and their applications. Discret. Math. Theor. Comp. Sci.: 46–71 (2001). https://doi.org/10.1007/978-1-4471-0673-9_4
9. Schmidt, K.:Quaternary constant-amplitude codes for multicode CDMA. IEEE Int. Symp. Inf. Theory: 2781–2785 (2007). https://doi.org/10.1109/isit.2007.4557639
10. Zhdanov, O. N., Sokolov, A. V.: A synthesis method of basic ternary bent-squares based on the triad shift operator. Syst. Anal. Appl. Inf. Sci. **1**: 77–85 (2017). https://doi.org/10.21122/2309-4923-2017-1-77-85
11. Trakhtman, A. M., Trakhtman, V. A.: Elements of Theory of Discrete Signals on Finite Intervals (1975)
12. Sokolov, A. V., Krasota, N. I.: Very nonlinear permutations: synthesis method for S-boxes with maximal 4-nonlinearity. Proc. ONAT **1**: 145–154 (2017). [Publication in Russian]
13. Maier, W.: Nonlinearity criteria for cryptographic functions. Adv. Cryptol. Eurocrypt. Lect Notes Comput. Sci.: 549–562 (1990). https://doi.org/10.1007/3-540-46885-4_53
14. Sokolov, A. V., Barabanov, N. A.: Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes, Radioelectron. Commun. Syst. **58**(5): 220–227 (2015). https://doi.org/10.3103/s0735272715050040
15. Logachev, O. A., Salnikov, A. A., Iashchenko, V. V.: Boolean functions in coding theory and cryptography. Am. Math. Soc. **241** (2012). https://doi.org/10.1090/mmono/241
16. Tokareva, N.: Bent Functions: Results and Applications to Cryptography (2015). https://doi.org/10.1016/b978-0-12-802318-1.00004-2