computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

PROPERTIES AND FORMATION OF OFDM AND DERIVED SIGNALS

Alexander Zamula [1], Vladyslav Morozov [1], Nataliya Kalashnykova [2], Robert Brumnik [3]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine, zamulaaa@gmail.com, ilissar@hotmail.com
[2] Tecnológico de Monterrey, Eugenio Garza Sada av. 2501, 64849 Monterrey, Nuevo León, México
[3] GEA College, Dunajska cesta 156, 1000 Ljubljana, Slovenia

Paper history:
Received 15 November 2018
Received in revised form 15 September 2019
Accepted 17 February 2020
Available online 14 June 2020

Keywords:
noise immunity;
information security;
broadband access;
cellular communication;
frequency division;
interference;
peak factor.

Abstract: The article discusses the technology of forming signals used in mobile, information and telecommunication systems, and also provides an analysis of promising technologies that can be used in wireless communication systems of broadband access. It is shown that the widely used modulation scheme with orthogonal frequency division (OFDM) has a number of drawbacks, which can lead to a decrease in system performance. Alternative technologies for generating signals are presented, in particular, a technology based on windowed signal processing (W-OFDM), a technology based on time division (w-OFDM); UFMC technology and others to eliminate the disadvantages of OFDM technology. New points of view are proposed on the use of multi-carrier transmission technology in the form of multiplexing with orthogonal frequency division (in order to increase the security of modern wireless broadband access communication systems from external and internal threats), a class of non-linear discrete cryptographic sequences to form a physical data carrier – signal.

1. INTRODUCTION

Modern wireless systems (for example, satellite systems, mobile telephony systems) belong to multi-user systems. When designing such systems, the main problem is to choose method of multiple access, i.e., the possibility of simultaneous use by many subscribers of a communication channel with minimal mutual influence [1, 2]. Broadband signals are widely used in modern high-speed cellular communication systems of the WiMax, Mobile WiMax, MBWA standards, wireless discrete communication systems, such as LTE and Wi-Fi, in the transmission of information from digital television (DVB-T) and radio (DRM, DAB), in radiolocation, etc. The use of signals with orthogonal frequency division multiplexing (OFDM), including specified information transmission systems, allows us to increase not only the information capacity of the system in case of multipath propagation with limited bandwidth, but also the data transmission speed, bringing it closer to the channel capacity, increase secrecy transmission capacity and noise immunity of the system. Currently, there is a rapid development, research and standardization of technologies for the fifth generation of cellular networks (5G). The most priority tasks in this direction are: to achieve the maximum data transfer rate (up to 20 Gbit / s), ensure the density of user devices (up to 10^6 devices / km2), provide users with highly reliable low latency communication services (URLLC) (with data transmission delay not more than 1 ms) [3-4]. In order to achieve the above objectives for 5G networks, the following are considered: use of the spectrum in the millimeter range [5]; new types of signal modulation and coding methods; multiple access methods; improved technologies for building antennas and networks architecture [5-6]. In addition, it is worth pointing out studies devoted to: orthogonal frequency division multiplexing with filtering (F-OFDM) [7-9]; spatial diversity technologies (MIMO) [10]; radiocommunication cloud networks (C-RAN) [11], orthogonal frequency division technology with coding (C-OFDM) [12] and many others.

2. OFDM TECHNOLOGY ADVANTAGES

The main idea of OFDM is to achieve a high transmission rate in the frequency domain, by dividing full signal frequency range into a number of non-overlapping frequency subchannels with lower speeds. In addition, each subchannel (subcarrier) is modulated by a separate symbol, then these channels are multiplexed in frequency domain and data are transmitted in parallel in orthogonal subchannels. Compared to single carrier transmission, this approach provides enhanced resistance to narrowband interference and channel distortion. Specified, in particular, allows for a high level of system flexibility, since modulation parameters, such as constellation size, coding rate, can be independently selected for each subchannel.

The widespread use of the OFDM digital modulation scheme is due to a number of remarkable features of this technology:

- resistance to multipath effects;
- high noise immunity to narrowband interference;
- resistance to intersymbol interference due to the fact that the duration of the symbol in the auxiliary subcarrier is significantly longer compared to the propagation delay than in traditional modulation schemes;
- high spectral efficiency in comparison with traditional systems with frequency division of channels due to the large number of subcarriers;
- the ability to use different modulation schemes for different subcarriers, which allows you to adapt to the conditions of signal propagation and to different requirements for the quality of received signals;
- simple implementation using digital processing methods, etc.

3. SECURITY INDICATORS EVALUATION

State level of informatization is determined primarily by the development of information communications, as a set of network resources intended for the production and provision of telecommunications, information and other services. The development of wireless communications technologies has been constantly shaped based on studies of waveforms. As an example, we can use the technology of multiplexing signals with orthogonal frequency division multiplexing in modern wireless broadband access systems (WiMAX, Wi-Fi, LTE, etc.). The use of this technology allows increasing the information capacity of the system with a limited bandwidth, data reception and transmission speed, bringing it closer to the channel capacity, increasing the secrecy transmission capacity and noise immunity of signal reception, and as a result, to meet the ever-increasing needs of network users in high-speed connections services.

Analytically, the OFDM signal can be represented as [13]:

$$S(t)=\sum_{k=0}^{N-1}S_k(t)=\sum_{k=0}^{N-1}A_{k^{e^{j2\pi kf/T}}},0\le t\le T, \quad (1)$$

where k is the subcarrier index, $S_k(t)$ is the signal on the k-subcarrier, A_k is the amplitude component of the sequence of information symbols, N is the number of subcarriers, T is the duration of the information symbol.

The block diagram of an OFDM modulator is presented in Figure 1 [14,15]. In the transmitter, the serial stream of binary symbols s[n] is encoded with an error-correcting code, interleaved further, using inverse multiplexing (demultiplexing), turns into N parallel streams, each of which is matched (complexly) with the output stream s[n] using certain constellation modulations (quadrature modulation QAM, quadrature phase modulation QPSK, etc.). The number of outputs of the demultiplexer is determined by the number of subcarrier frequencies. Next, the modulated $X_0,...,X_{N-1}$ symbol streams undergo a fast inverse Fourier transform, which translates them into digital responses $X_0,...,X_{N-1}$ (in general, complex numbers) in the time domain. The real ($R_e\{x_i\}$) and imaginary ($I_m\{x_i\}$) components of the response $x_i(i=0,...,N-1)$ are subjected to digital-to-analog conversion. The received analog signals are used for modulation in accordance with the sine wave and cosine wave (obtained by shifting the sine wave by 90) of the carrier frequency. After modulation, the signals are summed to form a signal s(t), which enters the communication channel.

Subcarriers orthogonality makes it possible to select each of them from the common signal at the reception even in the case of partial overlapping of their spectra. Since the subcarriers are located close to each other and even partially overlap, the spectral efficiency of the modulated OFDM signal is high. The parameters of the subcarrier signals are selected in such a way that they are orthogonal to each other, that is, the condition is met for them:

$$\int_0^T \sin 2\pi f_1(t)\sin 2\pi f_k(t)dt=0, \quad (2)$$

where t is the duration of the information symbol, f_l and f_k are the frequencies of the l-th and k-th subcarriers, respectively.

The orthogonality of the carrier signals guarantees the frequency independence of the channels from each other and, therefore, the absence of inter-channel interference. For the fast implementation of this procedure, the inverse fast Fourier transform algorithm is used, that is, the signal values at the input of the IFFT block belong to the frequency domain. At the output of the block IFFT receives the signal value in the time domain. Combining all the values, a complex OFDM signal is obtained. Taking into account the fact that IFFT works effectively with arrays of dimension 2k, the number of subcarriers is chosen with the same multiplicity. For example, in WiMAX wireless communication systems, the number of subcarriers is chosen from 128 to 2048 and can occupy frequency bands from 1.25 MHz to 20 MHz. For each of the subcarriers, a different modulation type is used depending on the requirements and the type of interference in the channel. At the receiving end, the inverse operations are performed, in this case, instead of a digital-to-analog converter, an analog-to-digital converter (ADC) is used, instead of a reverse FFT, direct FFT.

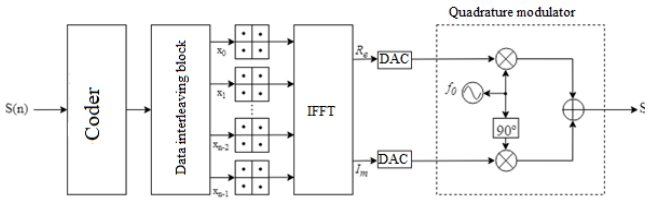

Figure 1 – OFDM modulator circuit

The structure of the OFDM signal can be quite complex because it consists of many components:

- the structure of the time-frequency distribution, given by: initial frequency, frequency grid pitch, number of subcarriers;
- time slots specified by: the duration of the symbol, the duration of the guard interval;
- type of manipulation: phase (BPSK, QPSK, 8-PSK) or amplitude-phase quadrature modulation (QAM)
- discrete sequences that determine the law (rule) of manipulating the phase of the high-frequency carrier, and given the dimension of the signal space;
- type of symbol sync;
- the presence and type of noise-resistant coding (Reed-Solomon code, Bowes-Choudhury-Hokvingem code, turbo codes, etc.)
- the presence and type of data interleaving and so on.

The above features of the OFDM signal structure can be used in the construction of ICT, for which the ensuring requirements of the specified security indicators against the introduction (imposition) of spurious messages, falsification of messages; data integrity, confidentiality, noise immunity of reception, operation secrecy are decisive.

One of the components of information security (along with information secrecy) is imitation protection (ensuring integrity) of information. The mathematical apparatus of the imitation protection system includes a cryptographic algorithm for simulating the encryption of information (this may be an encryption algorithm, an authentication code, or another transformation) and an algorithm for determining the truth of the information received, as well as a key system. In essence, imitational security is a complex service that is provided by such services as integrity, authenticity (truth), as well as the use of various cryptographic protocols with certain properties [14,15]. As studies [16,17] have shown, it is possible to provide the imitability necessary in ICS at the source level of complex signals by increasing the dimension of the signal space, the degree of correlation between them, the complexity of the laws of their construction. In accordance with the above definitions, the theory of authentication by J. Simons [18] can be used to quantify the simulated security. It was Symons who showed that for the quantitative assessment of authenticity one can use the probability P_{imp} of deception:

$$P_{imp} \geq 2^{-\Delta I(C,K)}, \qquad (3)$$

where $\Delta I(C,K)$ is the amount of information on the authentication key K entered into the C cryptogram.

Let us analyze the expression (3).

1. Systems in which equality (3) is achieved are referred to as systems that are absolutely resistant to deception.

2. To reduce the probability of fraud, it is necessary to increase $\Delta I(C,K)$.

Taking into account the peculiarities of the OFDM signal structure, imitability (I_c) depends on: the dimension of the signal space (I), the number of attempts (C) of imposing (simulating), the space (Z) of the component of the OFDM signal structure (in particular: initial frequency, frequency grid spacing, ensemble of discrete sequences (signals), number of subcarriers, etc.), imposition strategies (X):

$$I_c = F(I,Z,C,X). \qquad (4)$$

At the complex signals source level (physical level), the probability of cheating or imposing a false signal is defined as

$$P_{imp} \geq 2^{-l_i}, \quad (5)$$

where l_i is the length authentication code, the dimension of the signal space

Analysis of the data in Table 1 shows that the proposed method for the synthesis of complex non-linear discrete cryptographic signals allows for the formation of large ensembles of discrete sequences. So, for the period of the sequence N = 63 the number of pairs of CS satisfying the maximum value of the maximum PCCF side lobes - 17 is 12214869. For a representative of the class of linear sequences - sequences with a three-level cross-correlation function (Gold set), which are optimal from the point of view of cross-correlation functions [23], the number of pairs of signals corresponding to a given boundary is 975. The excess of the volume of a CS over an ensemble composed of M-sequences is more than 10^7 times.

Table 1 – Signal properties

Signal class	Sequence period	Dense packing value	Signal ensemble volume	Imp. Prob. value
M-seq.	31	9	3	$3\ 10^{-1}$
PCCF	31	9	495	$2\ 10^{-3}$
CS	31	9	1465137	$7\ 10^{-7}$
M-seq.	63	17	20	$5\ 10^{-2}$
PCCF	63	17	975	$1\ 10^{-3}$
CS	63	17	12214869	$8\ 10^{-7}$
M-seq.	127	27	36	$2\ 10^{-2}$
PCCF	127	17	11610	$8\ 10^{-5}$
CS	127	27	9006648	$1\ 10^{-7}$
M-seq.	255	36	28	$3\ 10^{-2}$
CS	255	36	17599	$5\ 10^{-5}$
M-seq.	511	63	276	$3\ 10^{-3}$
PCCF	511	33	147500	$6\ 10^{-6}$
CS	511	63	2666671	$3{,}7\ 10^{-7}$
M-seq.	1023	100	435	$2\ 10^{-3}$
PCCF	1023	65	338000	$3\ 10^{-6}$
CS	1023	100	5293538	$2\ 10^{-7}$

For the period of a sequence of 1023 elements, the number of pairs of gearboxes satisfying the limiting value for the side lobes of the cross-correlation function (CCF) 100 is 5293538, whereas for a representative of the class of linear sequences of M-sequences, the number of pairs that meet this boundary is 435, then there is an excess of the volume of the signal system is more than 105 times. With a slight decrease in the requirements for the limiting value of the maximum lateral peak of PCCF, according to which the selection of signals is carried out (in fact, a reduction in the noise immunity of reception), the performance of the ICS system can be significantly improved. So, for the period of the sequence N = 127, increasing the limit value by 1.2 dB will increase the ensemble volume from M = 11610 (at the border of 17) to 9006648 signals, with a limit value of 27, that is, 776 times. As follows from the data in Table 1, the probability values of imposing in the case of the application of the CS are much less. So, with a period of the sequence L = 1023, it is four orders of magnitude less than using M-sequences and an order of magnitude less than when using sequences with a 3-level PCCF. An improvement in the imitation resistance index of the ICS is achieved due to the fact that the CSs have improved ensemble properties in comparison with linear classes of signals, in particular, M-sequences. In Table 2 shows the results of calculating the statistical characteristics of various correlation functions for discrete signals widely used in communication systems, including the characteristics of cryptographic DS. Calculations were carried out for different values of the DS period. The statistical characteristics of the correlation functions were selected: the value of maximum lateral emissions $R_{\max}$, the value of the expectation of the emission module $m_{|R|}$, the value of the standard deviation of the emission module $D_{|R|}^{\frac{1}{2}}$ and emission values $D_{|R|}^{\frac{1}{2}}$.

Analysis of the data given in Table 2, suggests that maximum lateral emissions values of the CS, as well as the statistical characteristics of this class of signals are not inferior to the corresponding characteristics of the signals constructed using M-sequences and characteristic discrete signals [7-12, 21-31]. This, in turn, indicates that the use of a CS provides noise immunity for receiving signals no worse than when applying the decree of signals based on linear formation laws. According to the data in Tables 1-2, it also follows that by varying the limiting values of the side-lobe level of the correlation function, depending on the requirements for the ICS, the tasks of achieving the required values of the noise immunity indicators for signal reception, imitation resistance and secrecy of the ICS, can be solved.

Table 2 – Correlation function statistical characteristics

ST	Char-tics	$\frac{R_{\max}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D_{\lvert R\rvert}^{\frac{1}{2}}}{\sqrt{N}}$	$\frac{D_{(R)}^{\frac{1}{2}}}{\sqrt{N}}$
CDS	AACF	1,0 - 1,8	0,5	0,4	0,5
	PACF	0,1 – 1,9	0,2	0,1	0,2
	MIACF	1,4 - 2,6	0,6	0,5	0,8
	ACCF	1,9 - 3,2	1,0	0,8	1,0
	PCCF	2,5 – 3,6	1,0	0,8	1,2
	CCCF	2.1 – 5,0	0,9	0,7	1,1
M-seq	AACF	0,7...1,25	0,32	0,26	0,41
	PACF	$\frac{1}{\sqrt{N}}$	$\frac{1}{\sqrt{N}}$	0	0
	MIACF	1,3...2,3	0,66	0,49	0,82
	ACCF	1,4...5,0	0,54	0,48	0,73
	PCCF	1,9...6,0	0,8	0,62	1,0
	CCCF	2,0...5,1	0,83	0,62	1
CS	AACF	1,2 – 1,9	0,5	1	1,1
	PACF	0,2 - 1,9	0,6	0,4	0,7
	ACCF	1,4 – 3,4	0,5	0,4	0,6
	PCCF	1,9 – 5,2	0,7	0,5	0,8

Let us make an ICS protection assessment from imposing false messages, for the case when the system uses a dynamic shift mode (according to the law of the control sequence) correspondence: the message bit is a complex signal. In this case, the value of the probability of imposing a false message ($P_{imp/mes}$) (with equiprobable choice of characters of the control sequence) can be defined as:

$$P_{imp/mes} = (2^{-k})^n, \quad (6)$$

where: 2^{-k} a number of possible states of the source of the control sequence, which is determined by an ensemble of discrete signals of information carriers; n – message length provided in bits

Table 3 shows the values of the probability of imposing $P_{imp/mes}$ on the message for discrete signals obtained because of carrier manipulation according to the law of M-sequences, PCCF and nonlinear cryptographic sequence. The message size is n=32. In the calculations of $P_{imp/mes}$, for the case of application in the system of nonlinear CS, sequences were selected whose correlation characteristics are close to the optimal limit values from the point of view of PCCF ($R_{\max} \le \frac{1,5}{\sqrt{N}}$).

Table 3 – Imposter value for signal systems

Signal period	M-seq.	PCCF	nonlinear CS
31	2^{-96}	2^{-288}	2^{-672}
63	2^{-96}	2^{-320}	2^{-768}
127	2^{-160}	2^{-448}	2^{-640}
1023	2^{-192}	2^{-608}	2^{-736}

Data analysis in Table 3 shows that in ICSs, which apply signal multiplexing technologies in orthogonal frequency division of channels, the value of $P_{imp/mes}$ for nonlinear CS is much less than in the case of using linear classes of signals.

4. DERIVED CRYPTOGRAPHIC SIGNAL SYSTEMS SYNTHESIS

Among the systems of phase-shifted signals, many are based on Walsh systems [1]. It is known that the auto- and cross-correlation functions of the Walsh sequences have large side peaks. To improve signals correlation properties, derived signal systems (DSS) are formed by multiplying Walsh sequences (source sequences) by a signal that has certain properties (producing a signal), in particular, have small side peaks of the autocorrelation function.

The authors formulated a hypothesis about the possibility of using nonlinear cryptographic sequences as generating ones, the theoretical foundations of which are given in [24].

The method of synthesizing derived signal systems based on the use of CS includes the following steps.

1. The selection of M cryptographic sequences of a fixed period N, with the minimum values of the maximum side lobes (R_{max}.) ACPF.

2. A set of Walsh codes (matrix N·N) is formed, in which each row corresponds to a separate code.

3. Perform the multiplication of sequences (each of the lines of the Walsh code of the original sequences) on the cryptographic signal, forming N derived orthogonal signals.

4. Carry out a study of the correlation properties of the obtained derived orthogonal signals (in particular, ACPF, ACAF). To study the functions of cross-correlation, they form a matrix of dimension N·N. The number of such matrices: L·N.

Table 4 shows cryptographic sequences (M = 14), selected from a set of sequences, by the criterion of the minimum values of the maximum side lobes ACPF ($R_{max} < 10$).

Table 4. CS with minimal ACPF side lobes

1	11100011111010000111110111001100110001010001101011010011001001100101
2	10000100100001001011100110100000001100100100000101110011001110011101
3	00001001000010010111001101000000011001001000001011100111001110011011
4	00001001000010010111001101000000011001001000001011100111001110011011
5	00010010000100101110011010000000110010010000010111001110011001110110
6	01001000010010111001101000000011001001000001011100111001110011000
7	00001001011100110100000001100100100000101110011100111010001100010110
8	00010010111001101000000011001001000001011100111001110110001011101
9	00100101110011010000000110010010000010111001111001110110001011010
10	01001011100110100000001100100100000101110011001101110100011001010100
11	00000000101000100110000011111000011011011100011010000101111100101
12	00000001010001001100000111110000110110111000110100001011111001010
13	00000010100010011000001111100001101101110001101000010111100010100
14	01000111100011000001001100100000000110111110111001010110001010110

The results of the CCPF DSS study based on cryptographic sequences show that the number of pairs of signals for a period of sequences is 64 characters, for which the values R_{max} do not exceed 17 (this is the so-called «dense packing» border, achieved in the class of the best, from the point of view of CCF, sequences with a three-level CCPF), 604 pairs (about 30% of the total number of possible combinations of pairs of signals). The number of signals pairs for which values R_{max} does not exceed 20 – 1577, which is 77% of the total number of signal pairs. With limit $R_{max} < 25$ the maximum number of selected signal pairs is 1984 (96,8%). Such values R_{max} have a place for sequences that are most prevalent in modern telecommunications systems M-sequence.

Table 5 shows the results of studies of the correlation function statistical characteristics of various signal classes, including DSS, when used as generating cryptographic signals. As correlation function statistical characteristics were used: largest lateral emission values $\frac{R_{max}}{\sqrt{N}}$; expected value of the emission module $\frac{m_{|R|}}{\sqrt{N}}$; the value of the standard deviation of emissions $\frac{D^{\frac{1}{2}}_{(R)}}{\sqrt{N}}$ and emission module - $\frac{D^{\frac{1}{2}}_{|R|}}{\sqrt{N}}$. Calculations were carried out for different values of sequence periods (from 30 to 2052).

Table 5. Statistical characteristics of the correlation functions of various classes of signals

ST	Char-tics	$\frac{R_{max}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D^{\frac{1}{2}}_{\|R\|}}{\sqrt{N}}$	$\frac{D^{\frac{1}{2}}_{(D)}}{\sqrt{N}}$
NLCS	ACAF	1,6-2,4	0,3-3,4	1,4-7,7	1,9-10,8
	ACPF	0,02-0,5	0,02-0,3	0,03-0,3	0,06-05
	CCAF	1,3-3,3	0,5-0,7	2,4-18,2	3,6-27
	CCPF	0,8-3,3	0,7-0,8	5,8-45,3	5,9-45,3
DSS	ACAF	0,8-2,4	0,4-0,5	0,9-1	1-1,1
	ACPF	0,7-2,5	0,2-0,7	0,2-0,5	0,3-0,9
	CCAF	1-2,5	0,2-0,7	0,2-0,5	0,3-0,7
	CCPF	1,4-2,8	0,2-0,7	0,4-0,5	0,6-0,9
NLCCS	ACAF	0,7-2,5	0,4-0,5	0,9-1	0,9-1,2
	ACPF	0,9-2,5	0,3-0,7	0,2-0,5	0,3-0,9
	CCAF	1,2-2,7	0,4-0,7	0,3-0,5	0,5-0,7
	CCPF	1,5-2,8	0,5-0,7	0,3-0,5	0,8-0,9
Linear M-seq	ACAF	0,7-1,25	0,32	0,26	0,41
	ACPF	$\frac{1}{\sqrt{N}}$	$\sqrt{N}$	0	0
	CCAF	1,4-5,0	0,54	0,48	0,73
	CCPF	1,9-6,0	0,8	0,62	1

Analysis of the data given in Table 5, indicates that the values of the maximum lateral emissions of CS, as well as the statistical characteristics of this class of signals are not inferior to the corresponding characteristics of signals based on the use of M-sequences. As follows from the data presented in the table, the statistical characteristics of the DSS are close to the corresponding characteristics for linear and nonlinear signal classes. The values of the maximum lateral peaks of the DSS cross-correlation functions are smaller than those of the linear M-sequences widely used in modern ICS.

Due to the fact that CSs have ensemble properties that are improved compared to other classes of signals, ICS protection indicators against imposing (entering) spurious messages can be improved. At the same time, it should be noted that the use of CS ensures the noise immunity of receiving signals not lower than when applying the above signals based on the linear formation laws.

An assessment of security of ICS, protecting against false messages, is performed when

manipulating (extending the range) CS. At the same time, we will assume that the system implements a dynamic mode of operation, which implies, among other things, a change in the correspondence of m message bits - 2m complex signals. Change in compliance is made at set time intervals using a control sequence that meets the requirements of randomness. To provide the necessary noise immunity of signal reception, we will use CSs that have good correlation properties [1-2, 17].

The probability of imposing a false message is determined by the ability of the reaction station to determine the law of conformity: m bits of the message - 2m complex signals, or, in other words, determine the structure (law of formation) of the control sequence establishing the specified correspondence, and is determined from the ratio:

$$P_{imp./message} = (2^{-k})n, \qquad (7)$$

where: 2-k- the source control sequence possible states number; n – message length expressed in bits.

Note that the number of possible states of the source control sequence (2^{-k}) is determined by an ensemble of discrete sequences, by which the phase of the high-frequency carrier is manipulated to form a phase-shift keyed broadband discrete signal. Table 5 shows the values. $P_{imp./message}$ for various systems of discrete signals obtained on the basis of M - sequences, sequences with a three-level periodic cross-correlation function (CCPF), non-linear characteristic sequences (NLCS) and non-linear cryptographic sequences (NLCCS). The message dimension is set to n = 32. As the sequences period N were selected: 31, 63, 127, 1023.

It must be emphasized that in the calculations $P_{imp./message}$ (for use in the system NLCCS), sequences were selected whose correlation characteristics are close to optimal boundary values ("dense packing") from CCPF point of view. Such boundary values are achieved in a class of sequences with a three-level cross-correlation function and constitute $P_{side.\max} \le 1,5\sqrt{N}$.

Table 6. The message imposing probability values for different discrete signal systems

Sequence period (N)	$P_{imp./message}$ values for systems:		
	M-sequence	Sequences with CCPF	NLCCS
31	2^{-96}	2^{-288}	2^{-672}
63	2^{-96}	2^{-320}	2^{-768}
127	2^{-160}	2^{-448}	2^{-640}
1023	2^{-192}	2^{-608}	2^{-704}

As it can be seen from the data table, the values $P_{imp./message}$ for NLCCS are significantly smaller than in the case of using the most widely used in practice linear classes of signals (M-sequences and sequences with three-level CCPF). In the case when the system does not have strict requirements for the Pimp./message (imitation resistance), but it is necessary to provide increased requirements for signal reception noise immunity and to fulfill high requirements in terms of the structural secrecy of the complex signals used, the values of the maximum lateral peaks of the CCPF can be selected as the limiting values "dense packing". In this case, the volume of the system of signals satisfying this boundary will "be less, and accordingly $P_{imp./message}$ will be higher, but at the same time, the noise immunity of receiving signals will be improved. Thus, when using systems of nonlinear signals, it becomes possible to vary (taking into account the requirements for ICS) indicators of the noise immunity of signal reception — the system is protected from unauthorized data modification (imitation resistance).

The above estimates suggest that in ICS, in which as a method of information exchange, the dynamic mode of changing the correspondence is implemented, m bits of the message - 2m complex signals and apply nonlinear cryptographic signals, provide high levels of system security against unauthorized data modification and the imposition of false information.

In essence, the presented system of providing imitability is [18] a cryptographic system, because it contains all the attributes of such a system: an algorithm for protecting against imposing a false message and hiding the semantic content of a message, which is based on the implementation of the dynamic mode of ICS functioning using cryptographic discrete signals as information carriers; algorithm for indentifying the authenticity of the information received; a key system that implements the functions of generating a control sequence for a change of correspondence: the message bit is a complex signal, as well as the generation of cryptographic discrete signals.

The research results may be useful in other applications of modern computer and telecommunication systems [9-13, 18], for example, to optimize computing [21, 32-36], cryptography [20, 28-30], etc.

5. CONCLUSION

This paper presents the technologies for generating signals that are already used in communication and telecommunication systems, and also provides an analysis of promising technologies that may be used in various new systems, including

wireless broadband access communication systems, in particular derived cryptographic signals.

Studies of the DSS properties formed on the basis of nonlinear cryptographic sequences show that more than 30% of the total number of combinations of such DSS pairs have side peaks of the correlation function equal to potentially achievable values, for the remaining pairs the maximum side peaks of CF are less than in widely used linear M sequences. In addition, the resulting DSSs have improved structural and ensemble properties compared with orthogonal signals.

Currently, mathematical model and software have been developed that implement methods for synthesizing and studying the properties of non-linear cryptographic signal systems, which are almost available for possible use as part of prototypes and elements of modern digital communication tools, and allow us: to generate non-linear cryptographic signals for almost any period; determine the values of the minimum and maximum lateral emissions of various correlation functions; compare the obtained values with known, potentially achievable boundaries for the corresponding correlation functions; assign to the implementations of the synthesized sequences, as well as the parameters used for the synthesis of signals, unique identifiers that are necessary for optimal signal processing; calculate the statistical characteristics of the various correlation functions of the synthesized signals; carry out studies of the ensemble characteristics of the synthesized signals.

6. REFERENCES

[1] V.P. Ipatov, *Spread Spectrum and CDMA. Principles and Applications*, John Wiley & Sons Ltd, 2005.

[2] H. F. Arrano and C. A. Azurdia-Meza, "OFDM: today and in the future of next generation wireless communications," *Proceedings of the 2016 IEEE Central America and Panama Student Conference (CONESCAPAN)*, Guatemala City, 2016, pp. 1-6.

[3] ITU-R, Recommendation M.2083-0, *IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, ITU Recommendation, Sept. 2015.

[4] P. Guan et. al., "5G field trials: OFDM-based waveforms and mixed numerologies," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1234-1243, March 2017.

[5] T. S. Rappaport, et al., "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335-349, 2013.

[6] J.G. Andrews, et al., "What will 5G be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065-1082, June 2014.

[7] J. Abdoli, M. Jia, and J. Ma, "Filtered OFDM: A new waveform for future wireless systems," *Proceedings of the IEEE 16th International Workshop on Signal Process. Adv. Wireless Commun. (SPAWC)*, Stockholm, Sweden, Jun. 2015, pp. 66–70.

[8] X. Zhang, M. Jia, L. Chen, J. Ma and J. Qiu, "Filtered-OFDM - enabler for flexible waveform in the 5th generation cellular networks," *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, 2015, pp. 1-6.

[9] J. Li, K. Kearney, E. Bala and R. Yang, "A resource block based filtered OFDM scheme and performance comparison," Proceedings of the IEEE International Conference on Telecommunications ICT'2013, Casablanca, 2013, pp. 1-5.

[10] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590-3600, Nov. 2010.

[11] "C-RAN: The road towards green RAN," *China Mobile Research Institute, white paper*, 2011. [Online] Available at: http://labs.chinamobile.com/cran/

[12] H. Nikopour, et al., "Sparse code multiple access", *Proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, (PIMRC'2013)*, Sept. 2013, pp. 332-336.

[13] S. Vukotić and D. Vućić, "Detection and clasiffication of OFDM/QAM and OFDM/OQAM signals based on cyclostationary features," *Proceedings of the* 2015 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, 2015, pp. 232-235. DOI: 10.1109/TELFOR.2015.7377455

[14] M. G. Bakulin, V. B. Kreyndelin, A. M. Shloma, A. P. Shumov, *OFDM Technology. Textbook for universities*, Hotline-Telecom, 2015, 360 p. (in Russian)

[15] A. Manosueb, J. Koseeyaporn and P. Wardkein, "An adaptive demodulation for OFDM signal," *Proceedings of the 2016 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, Phuket, 2016, pp. 1-6.

[16] B. Sklar, *Digital Communications: Fundamentals and Applications, Prentice Hall Communications Engineering and Emerging Techno*, Pearson Education, 2016.

[17] G. Miao, J. Zander, K.W. Sung, B. Slimane, *Fundamentals of Mobile Data Networks*, Cambridge University Press, 2016.

[18] I.D. Gorbenko, A.A. Zamula, V.L. Morozov, "Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts," *Telecommunications and Radio Engineering*, vol. 76, issue 19, pp. 1705-1717, 2017.

[19] M. Kustra, K. Kosmowski and M. Suchański, "Hybrid sensing method of real OFDM signal," *Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS)*, Warsaw, 2018, pp. 1-6.

[20] G.J. Simmons, "Authentication theory/Coding theory," in: Blakley G.R., Chaum D. (eds) *Advances in Cryptology, CRYPTO'1984, Lecture Notes in Computer Science*, vol 196. Springer, Berlin, Heidelberg, 1985, pp. 411-431.

[21] V. Krasnobayev, A. Kuznetsov, S. Koshman, S. Moroz, "Improved method of determining the alternative set of numbers in residue number system," in: Chertov O., Mylovanov T., Kondratenko Y., Kacprzyk J., Kreinovich V., Stefanuk V. (eds) *Recent Developments in Data Science and Intelligent Analysis of Information. ICDSIAI 2018. Advances in Intelligent Systems and Computing*, vol 836. Springer, Cham, 5 August 2018, pp. 319-328. DOI: 10.1007/978-3-319-97885-7_31

[22] F. He, H. Man, D. Kivanc and B. McNair, "EPSON: Enhanced Physical Security in OFDM Networks," *Proceedings of the 2009 IEEE International Conference on Communications*, Dresden, 2009, pp. 1-5.

[23] F. Huo, G. Gong, "A new efficient physical layer OFDM encryption scheme," *Proceedings of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM'14)*, 2014, 1024-1032.

[24] I.D. Gorbenko, A.A. Zamula, A.E. Semenko, V. L. Morozov, "Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes," *Telecommunications and Radio Engineering*, vol. 76, issue 18, pp. 1581-1594, 2017.

[25] J. Guerreiro, R. Dinis and P. Montezuma, "Equivalent nonlinearities for studying nonlinear effects on sampled OFDM signals," *IEEE Communications Letters*, vol. 19, no. 4, pp. 529-532, April 2015.

[26] Sverdlik M. B., *Optimal Discrete Signals*, Moscow: Radio i svyaz', 1975, 200 p. (in Russian)

[27] O. B. Wojuola, "Cross-correlation index and multiple-access performance of gold codes in a spread-spectrum system," *Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon-si Gangwon-do, Korea, 2018, pp. 764-768.

[28] O. Karpenko, A. Kuznetsov, V. Sai, Yu. Stasev, "Discrete signals with multi-level correlation function," *Telecommunications and Radio Engineering*, vol. 71, issue 1, pp. 91-98, 2012.

[29] N.I. Naumenko, Yu.V. Stasev, A.A. Kuznetsov, "Methods of synthesis of signals with prescribed properties," *Cybernetics and Systems Analysis*, vol. 43, issue 3, pp. 321-326, May 2007.

[30] Yu.V. Stasev, A.A. Kuznetsov, "Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes," *Cybernetics and Systems Analysis*, no. 3, pp. 47-57, May-June 2005.

[31] S. Haykin, D. J. Thomson, J. Reed, "Spectrum sensing for cognitive radio," *Proceedings of IEEE*, vol. 97, pp. 849-877, 2009.

[32] Runovski, K., & Schmeisser, H. -. (2004). On the convergence of fourier means and interpolation means. Journal of Computational Analysis and Applications, 6(3), 211-227.

[33] V. Meena, V. Arvind, P. Vijayalakshmi, V. Kalpana and J. S. Kumar, "Optimized task clustering for mobile cloud computing using Workflowsim," *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, 2018, pp. 1000-1005.

[34] Bondarenko, S., Liliya, B., Oksana, K., & Inna, G. (2019). Modelling instruments in risk management. International Journal of Civil Engineering and Technology, 10(1), 1561-1568.

[35] Chornei, R., Hans Daduna, V. M., & Knopov, P. (2005). Controlled markov fields with finite state space on graphs. Stochastic Models, 21(4), 847-874. doi:10.1080/15326340500294520

[36] Tkach, B. P., & Urmancheva, L. B. (2009). Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition. Nonlinear Oscillations, 12(1), 113-122. doi:10.1007/s11072-009-0064-6

Alexander Zamula, *Doctor of Sciences (Engineering), Professor of the Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: discrete signals in information and telecommunication systems.*

Vladyslav Morozov, *postgraduate student, Faculty of Computer Science, Department security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: information technology in education, information security.*

Nataliya Kalashnykova, *Ph.D., Associate Professor of the Universidad Autonoma de Nuevo Leon, San Nicolas de los Garza, Mexico. Scientific interests: information theory and coding, security information systems and technologies.*

Robert Brumnik, *Ph.D., Professor Assistant, GEA College, Ljubljana, Slovenia. Areas of scientific interests: security information systems and technologies.*