INFORMATION AND COMMUNICATION SYSTEMS BASED ON SIGNAL SYSTEMS WITH IMPROVED PROPERTIES BUILDING CONCEPT

Gorbenko Ivan[1[0000-0003-4616-3449]], Zamula Alexander[2[0000-0002-8973-6190]], Morozov Vladyslav[3[0000-0003-0427-0107]]

[1]V.N. Karazin Kharkiv National University, Svobodu square 4, Kharkiv, 61022, Ukraine
gorbenkoi@iit.kharkov.ua
[2]V.N. Karazin Kharkiv National University, Svobodu square 4, Kharkiv, 61022, Ukraine
zamylaaa@gmail.com
[3]V.N. Karazin Kharkiv National University, Svobodu square 4, Kharkiv, 61022, Ukraine
ilissar@hotmail.com

Abstract. The paper presents the results of solving the actual problem of improving the performance indicators of information and communication systems (ICS), in particular, information security, noise immunity, secrecy, in terms of external and internal disturbing influences, based on the models and methods development for information exchange in ICS, synthesis new classes of nonlinear discrete cryptographic signals (CS) with the necessary properties. For the first time, complex non-linear discrete CS synthesis problem was formulated and solved, based on the use of random (pseudo-random) processes. Taking into account the requirements of cryptographic robustness and the complexity of generating a cryptographic signal as a source of random (pseudo-random) processes, the choice of a symmetric block encryption algorithm with a counter is grounded. The synthesis method obtained by the authors makes it possible to form large ensembles of discrete sequences of practically any period with given, but physically realizable, side-lobe values of auto, cross and butt correlation functions, as well as statistical characteristics of correlation functions that are not inferior to those of the best linear classes of signals, in terms of correlation functions. A method for synthesizing derived signal systems based on nonlinear discrete cryptographic signals is proposed. Improved (as compared with the known linear signal classes) ensemble, correlation and structural properties of the synthesized signal system allow improving the indicators of information security, noise immunity and secrecy of the operation of ICS.

Keywords: information security, secrecy, correlation function, complex signal, cryptographic signal, ensemble signals.

1 Introduction

In the context of intensive information counteraction by the parties, the interests and competition of which can be manifested in various fields, including, as recent events have shown, in the field of information and hybrid wars, the availability and use of secure information and communication systems (ICS) is of particular importance. To a significant extent, such systems are based on the use of secure radio channels. In this case, under system protection we will understand, in a broad sense, their ability to provide the necessary indicators for noise immunity, information, energy and structural secrecy. Increased requirements for the effectiveness of the ICS in the conditions of internal and external influences are largely not taken into account by existing information technologies. There is a contradiction between the stringent requirements for ensuring the reliability, secrecy, confidentiality, integrity, authenticity of data transmitted over wired and wireless ICS communication lines, and existing models, methods and technologies for managing telecommunications networks, information security, services and quality of service.

New models, methods and technologies creation for managing telecommunication networks, information security, services and quality of service, in order to improve system performance indicators, under external and internal impacts (threats), through the creation of various interferences (retransmitted, structural, impulse, broadband, narrowband etc.), breaches of confidentiality, integrity and authenticity of information exchange, are, in our opinion, relevant research areas.

A significant number of ICS are multi-user systems. In such systems, multiple channels are located within a common time-frequency resource. One of the most promising ways of multiple access to services and system resources is code division multiple access in the common frequency band (CDMA). This access method is the most promising in many aspects: high noise immunity of the channels and ensuring the confidentiality of the transmitted data; high transmission rate and bandwidth efficiency; high energy efficiency and network subscriber capacity. Since the code division of ICS channels is based on the difference in signals provided to system subscribers, the construction of such systems and their characteristics are determined by the choice of signals and their properties. A promising direction for ensuring the security of information resources is the use of distributed spectrum technology (broadband noise-like signals).

The main ways to solve the above contradiction is to increase the noise immunity (in particular, energy and structural secrecy, noise immunity of signal reception) and information security of ICS by improving the methodological basis for constructing ICS by developing information exchange methods, methods for synthesizing new classes of nonlinear complex discrete signal-data carriers with the necessary ensemble, correlation and structural properties.

2 Statement and problem solution for nonlinear discrete complex cryptographic signals system synthesis

The process of choosing complex signals structures that are rational for some criteria is identical to the synthesis of the corresponding manipulating discrete sequences (DS). As a criterion for choosing a discrete signal class, as a rule, they are guided by the criterion of minimum mutual interference (minimax criterion). Such a criterion implies the ensemble signal construction with volume M, manipulated by DS, which differ as much as possible from each other during possible cyclic shifts. The quantitative measure of the differences between manipulating DSs are the maximum ensembles side-lobe levels of the periodic autocorrelation function (ACPF) and the side lobe level of the periodic cross-correlation function (CCPF). On this basis, the broadband signals (BBS) used in ICS should have such correlation properties, when the lateral peaks of the correlation functions of the BBS are as low as possible, i.e. ideally should aim for zero. However, the requirement of ideality (zero values of side peaks) of auto- and cross- correlation functions between all cyclic shifts of K sequences and various signal system isomorphisms with period N is not feasible, since the values of side peaks cannot fall below 1/2√B (B – signal base) [1].

Information exchange methods used in ICS, as well as classes of wideband signals, used as a physical carrier of data (sets of linear recurrent sequences (M-sequence), Kasami, Golda, Kamaletdinov and others), possessing relatively small values of side lobes of auto- and cross-correlation functions that do not support necessary (for critical ICS applications) information security and noise immunity indicators [1]. Thus, in the process of information exchange in ICS for a long time, the correspondence: the message-signal bit is fixed, and the above signals have low structural secrecy, limited ensemble properties, and also exist only for a limited number of signal period values. In the case of period truncation (increase) of such signals, their correlation properties deteriorate.

The analysis showed that currently there are no regular methods for the discrete sequences (DS) synthesis that are optimal by the minimax criterion. The problem of DS synthesis turns out to be even more complex if the requirements are imposed on signal system dimension (volume), structural properties and the number of DS elements. Since, for distributed spectrum technology, data carrier signal properties are completely determined by DS properties, which manipulate the information bits of system users [1-2], the search for efficient methods for the discrete signals (sequences) synthesis of corresponding to the potentially achievable boundary characteristics of correlation functions (minimax properties) or the border of “dense packing”) and possessing the required correlation, structural, ensemble properties.

The quality of services provided by ICS is proposed to assess, including the level of information security. At the same time, information security means the ability of ICS to provide protection against the destruction, modification, blocking of information, its unauthorized leakage or against violation of the established procedure for its routing. Also, information security should be understood as the state of security of data processing and storage systems, which ensures information confidentiality, integrity and availability, as well as other information properties and services: authenticity, traceability, irrefutability and reliability. [3].

We will formulate in general terms the problem of signal synthesis with given correlation ensemble and structural properties that provide the required values of noise immunity, information security and information transmission system secrecy. We require that such signal systems have the property of "blurring" in the correlation properties. This property means that increasing or decreasing the length of a discrete sequence does not change the correlation properties of the original discrete sequence.

The need to use secure radio channels forces researchers to take a fresh look at both protected radio channels operation modes and formation and application of complex signals aspects. Therefore, in our opinion, new approaches and new views on the complex signals application processes and functions are needed. In our opinion, new fundamental understanding of methods to ensure information secrecy, that is, functions that in traditional ICS are assigned to cryptographic systems and means. Therefore, a productive step, from the point of view of a new direction of using complex signal systems, is the synthesis of so-called cryptographic signal (CS) systems. The synthesis of such signals is based on the application of key data, and at the same time, the signals must have: absolute structural secrecy regarding the laws of their formation; improved ensemble properties (exist for almost any period value, have a significant amount of signal system); necessary to ensure the required value of noise immunity, the correlation properties. For protected radio channels, considered signal systems are defined by the applications in which they applied. In particular, these can be either individual signals or pairs of signals, as well as large sets of discrete sequences with necessary, but objectively limited values of «dense packing», cross-correlation and ensemble properties.

Under cryptographic discrete signals, it is proposed to understand symbol sequence sets (vectors) of a certain alphabet that possess the necessary (specified) structural, ensemble and correlation properties, temporal and spatial formation complexity and are formed on the basis of random (pseudo-random) processes, including using cryptographic algorithms [4-6]. Such signals must meet the requirements of chance, irreversibility, unpredictability [7], have correlation and ensemble properties determined by the owner (user) ICS. The use of CS, will improve the performance of ICS, in particular: noise immunity (noise immunity of signal reception in the face of structural, barrage, retransmitted and other types of interference, secrecy of operation) and information security. With this approach, the signal's structural secrecy is provided by randomness or pseudo-randomness of the symbol sequence, noise immunity is provided by the synthesized signal system correlation properties, ICS information security is provided based on statistical properties of CS close to the properties of random sequences, and the use of cryptographic keys, and the key length can be significantly less than the period (length) of the signal itself. It is necessary to note the special property of cryptographic signal systems: the possibility of their recovery in space and in time using keys and a number of other parameters that are used in the synthesis of this signal system.

3 Discrete cryptographic signal models

Under task of constructing (synthesizing) CS, we will understand the task of constructing subsets of discrete sequences. $(W_l^q), q=\overline{1,N}, l=\overline{1,L}$, the combination of which forms a discrete signal system with given dimension alphabet $M_k = N \times L$, such that in each of the subsets (vocabulary) the conditions that are imposed on the subset of CS in terms of structural, ensemble, correlation properties, spatial and temporal complexity of their generation are met.

CS construction is based on the analysis and use of periodic and aperiodic correlation functions and is based on the following theoretical principles.

1. Ensuring conditions for fulfilling the requirements for structural and ensemble properties, the possibilities of forming a CS subset with permissible temporal and spatial complexity, including using keys.

2. CS formation W^q, periodic autocorrelation function (ACPF) of each of which satisfies the system of nonlinear parametric inequalities (NPI):

$$R_{a_1}^{q}(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R_{a_2}^{q}(l),\ l=\overline{1,L-1},\ q=\overline{1,N}, \qquad (1)$$

where $R_{a_1}^{q}(l)$ i $R_{a_2}^{q}(l)$ – ACPF implementation setpoints, and indices are calculated modulo *(i+ l) modL.*

If $l=L$ for all $q=\overline{1,N}$ (1) convolution by value L

$$\sum_{i=0}^{L} W_i^q W_i^q = L, q=\overline{1,N}. \qquad (2)$$

3. Pair formation CS W^q and W^p, cross-correlation functions (CCF) which meet the requirements that are determined by a set of NPI systems (3), and also meet the requirements for butt cross-correlation functions (CCBF) pair CS W^q and W^p with butt discrete signals W^{qp} and W^{pq} (3 – 7):

$$R_{b_{l,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l) \qquad (3)$$

$$R_{b_{l,2}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l); \qquad (4)$$

$$R_{b_{l,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l); \qquad (5)$$

$$R_{b_{l,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l); \qquad (6)$$

$$R_{b_{l,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l); \qquad (7)$$

where $l=\overline{1,L-1}$ for all kinds of connections q and p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q \neq p$, where $R_{b_{1,j}}^{qp}(l)$ and $R_{b_{2,j}}^{qp}(l)$, CCPF and CCBF implementations are set respectively, $j=\overline{1,5}$.

In NPI systems (1) - (2) and (3) – (7) W_i^q and W_i^p are unknown values of random or pseudo-random characters CS W^q and W^p, $q=\overline{1,N}$, to be determined in the process of their construction.

Let us analyze the systems of nonlinear parametric quadratic inequalities (further - systems) (1) - (2) and (3) - (7), using the introduced model·

Systems (4) and (6) if $l=L$ for all $q=\overline{1,N}$ must give a complete convolution with the value L, i.e (4):

$$\sum_{i=1}^{L} W_i^q W_i^q = L, q = \overline{1,N} \quad (8)$$

and (6) gives

$$\sum_{i=1}^{L} W_i^p W_i^p = L, p = \overline{1,N}\,. \quad (9)$$

Systems (3), (5) and (7) with *l=L* for all pairs W^q and W^p give the values of the cross-correlation function at the zero value of the shift of the corresponding type:

$$\sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0); q, p = \overline{1,N}, \quad (10)$$

$$\sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), q, p = \overline{1,N}, \quad (11)$$

$$\sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), p, q = \overline{1,N}\,. \quad (12)$$

In the following, systems (1–2), (3–7) and the quadratic equation (10) will be called the subset (dictionary) model CS.

We will analyze the systems (1), (2) for the existence of solutions and independence. Directly from (1) it follows that for each of *q* CS there *L* unknown - $W_1^q, W_2^q \cdots W_L^q$. To find them according to (1), you can make a system of *L-1* independent NPI. Further, using (2), we obtain one more expression, but already the equality. A feature of system (1) is that it gives a convolution of each of *q* CS with value *L*. Based on (1) and (2), each N subset of CS can be constructed to form N independent systems of quadratic NPI, each of which will contain *L-1* quadratic inequalities of the form (1) and formally one equality, so that all of them will be *L*.

We will also analyze the totality of systems of parametric inequalities (3-7), taking into account (8) – (12), for solutions existence, systems independence and individual equalities. Systems (3-7) determine the permissible cross-correlation properties with respect to the CCPF and CCBF of each pair CS – W^q and W^p. They define the requirements for CCPF and butt cross-correlation functions (CCBF) specifically only two CS -W^q and W^p. When building three CDSs, we'll have 3!/2 systems like (3-7), and for N CS respectively -*N!/2* such systems. Thus, with increasing N, the number of systems of the form (3-7) increases exponentially (in terms of factorial).

For N = 2, among (8) – (12) NPI systems are redundant nonlinear quadratic equalities. Equality (2) coincides with (8) and (9), therefore, the last two are already included in system (2), are dependent, and therefore cannot be used. Further, equalities (10) and (11) coincide, and equality (12) is symmetric, in terms of the correlation function, with respect to equalities (10) and (11). Therefore, for each pair *p* and *q* independent is (10).

Based on a detailed analysis, we find that all (3-7) NPI systems define different implementations of CCPF and CCBF specifically only two CS W^q and W^p. Therefore, a mathematical model for constructing two CS W^q and W^p uniquely determined by the five systems NPI like (3 -7), and, as already stated, by the equation (10).

The above analysis results allow us to determine model complexity and, on its basis, *N* CS subset constructing.

1. When building a CS, it is necessary, depending on the allowed values. $R^{q}_{a_1}(l)$ and $R^{q}_{a_2}(l)$, which are determined by the boundaries of «dense packing», consider $v \geq k$ systems such as (1 – 2).

2. When building two CS you need to consider $v_2 \geq k_2$ systems like (3 – 7), where k_2 determined by $R^{qp}_{b_{1,j}}(l)$ and $R^{qp}_{b_{2,j}}(l)$.

3. When building N CS you need to consider $v_N \geq k_N$ systems like (3-7), where k_N determined by $R^{q}_{a_1}(l)$, $R^{q}_{a_2}(l)$ and $R^{qp}_{b_{1,j}}(l)$, $R^{qp}_{b_{2,j}}(l)$ valid values.

Thus, on the basis of taking into account the boundaries of CS subset [1,6] physical packing, there are possibilities for constructing subsets of CS in accordance with (1 -2) and (3 -7). Similarly (1 -2) and (3- 7) the model of the CS subset (dictionary) is specified through aperiodic autocorrelation functions (ACAF). In this case, simplifications are possible. So, the system (1 -2) by analogy can be represented as the NPI system based on aperiodic correlation functions, i.e.

$$r^{q}_{a_1}(l) \leq \sum_{i=1}^{L-m} W^{q}_{i}\left(W^{q}_{i+1}\right)^{*} \leq r^{q}_{a_2}(l),\ l=\overline{1,L},\ m=\overline{1,L}, \tag{13}$$

where $r^{q}_{a_1}(l)$ and $r^{q}_{a_2}(l)$ – given but admissible implementations in terms of «dense packing». Systems (1 - 2) and (3- 7) can also be represented through aperiodic cross-correlation functions (CCAF) as a system NPI

$$r^{qp}_{b_{1,1}}(l) \leq \frac{1}{L-m}\sum_{i=0}^{L-m} W^{q}_{i}\left(W^{q}_{i+1}\right)^{*} \leq r^{qp}_{b_{1,2}}(l); \tag{14}$$
$$l=\overline{1,L},\ m=\overline{1,L},$$

$$r^{qp}_{b_{2,1}}(l) \leq \frac{1}{L-m}\sum_{i=0}^{L-m} W^{p}_{i}\left(W^{q}_{i+1}\right)^{*} \leq r^{pq}_{b_{2,2}}(l); \tag{15}$$
$$l=\overline{1,L},\ m=\overline{1,L},$$

where $r_{b1,1}{}^{qp}, rr_{b1,1},{}^{qp}\ r_{b2,1},{}^{qp}\ r_{b2,2}{}^{qp}$ - permissible in terms of «dense packing», ACAF and CCAF.

4 Solution for CS subset constructing (synthesis) problem

The authors first obtained complex non-linear cryptographic signal systems synthesis method. The construction (synthesis) of CS sets is based on the application of key data, as well as random or pseudo-random processes. The method includes the following steps. [6].

1. Discrete sequences formation using key data and a source of random (pseudo-random) processes.
2. Potential CS statistical properties evaluation [7].
3. Build the required number of potential CS W^q using the system (1) and key data.
4. Finding pairs or subsets CS W^q and W^p, that meet the requirements (3 – 7).
5. Obtaining a cross-correlation functions state matrix of all possible pairs of potential CS, selected by the results of the previous step, and have all the necessary properties.
6. Processing the matrix, consisting in the fact that the formation of the required number of subsets or pairs CS according to (1) and (2) and selection into a subset of sequences satisfying the boundaries «dense packing» (maximum achievable values) for the corresponding correlation functions.

In order to ensure cryptographic security and structural secrecy (complexity) of cryptographic signals, the choice of a symmetric block encryption algorithm with a counter is justified as a source of pseudo-random sequences of characters (1st stage of the method): National cryptographic standard of the block symmetric transformation DSTU 7624:2014, defining the cipher «Kalina» and its modes of operation to ensure the confidentiality and integrity of information [8]. Alternatively, such a source may be offered a source based on the AES algorithm (international standard ISO/IEC 18033). Preference is given to choosing DSTU 7624:2014, taking into account the following factors. Block symmetric ciphers are one of the most common cryptographic primitives. In addition to ensuring the confidentiality (encryption) of the main volumes of information transmitted over the network or stored locally, they are used as a constructive element of other primitives (hashing functions, message authentication codes, pseudo-random sequence generators, etc.). The significance of this cryptographic transformation is underlined by a number of international contests, such as AES, NESSIE, CRYPTRACK, which were focused on the development of block cipher (as the main goal or as part of a set of promising solutions).

The national standard supports the block size and encryption key length of 128, 256, and 512 bits (the key length is equal to the block size or twice its size), providing a normal, high, and extremely high level of resilience (now it is the only block encryption standard in the world that supports 512 bit symmetric keys). Different standard versions provide flexibility in the choice of parameters for developers of cryptographic protection systems, which makes it possible to obtain both the highest level of performance and the greatest margin of transformation durability. High-level design uses well researched Square-like SPN-structure, used in algorithms AES/Rijndael, Whirlpool, «Stribog» and many others. The cycle transformation is built on the basis of lookup tables (S-blocks) and multiplication by an MDR-matrix over a finite field, providing the necessary cryptographic properties. The use of such design allows us to provide provable durability with respect to differential, linear and other types of cryptographic analysis, while simultaneously providing an efficient implementation for a wide range of software and hardware-software platforms. When choosing the size of the MDR-matrix, the size of the L1 cache of modern and promising processors was taken into account, which made it possible to optimize the speed of the software implementation of the cipher. Ukraine standard provides the greatest non-linearity of Boolean functions, which gives an additional margin of stability with respect to linear cryptanalysis. In addition, in our opinion, the standard of the block symmetric transformation DSTU 7624:2014 refers to post-quantum algorithms, i.e. - it will provide (at the choice of the corresponding parameters) cryptographic resistance against attacks with the use of quantum computers.

Finding discrete sequences with the necessary correlation functions characteristics is reduced, in fact, to the enumeration of all possible variants of the sequences belonging to a certain set and the selection of those sequences that satisfy the known estimates. Moreover, the computational complexity of such methods turns out to be quite significant. It is known that there is a large group of improved brute force methods, united by the common name «branch and bound method» [9]. The main idea of such methods is to use the finiteness of the set of solutions and to replace their complete search with a reduced (directed) search. Thus, the essence of improved brute force methods is to find optimal solutions for various optimization problems, in particular, discrete and combinatorial optimization. For method implementation procedure for finding estimates (boundaries) being used. The procedure for finding estimates is to establish the boundaries for solving the problem of finding valid values. If the estimate of the subset (parameter) is greater than the boundary of the values of the function of the subset, then the value is excluded from further consideration. The general principle implementation described above has certain difficulties determined by the specifics of the optimization problem being solved. As applied to the problem of synthesizing systems of nonlinear discrete cryptographic signals formulated above, this optimization method is aimed at implementing the procedure «branching», consisting in splitting the set of permissible values of a variable x (scan steps) on subregions (subsets) of smaller sizes. The resulting subregions form a tree called the search tree or the tree of branches and borders. The nodes of this tree are constructed subregions (subsets of the set of values of the variable x). In the course of the research, the authors obtained an improved method for the synthesis of nonlinear cryptographic sequences based on the use of an abbreviated (directed) search based on the application of the method «branches and borders», by excluding from further consideration subregions (implementations of discrete sequences that have side lobes of the correlation function that exceed the boundary established by the researcher), as well as using the properties and mutual relation of ACAF and ACPF, as well as «big» and «small» steps. Simulation modeling of the above sequence synthesis method was carried out and the performance (speed) of which was estimated. As the source of nonlinear cryptographic signals, the data encryption standard of Ukraine «Kalina» was used. In the modeling process, using the above method, sequences were selected with different symbol repetition periods (from 256 to 1024), whose autocorrelation function meets «dense packing» boundary for specified periods. Analysis of the research results showed that this method provides a performance gain in nonlinear discrete cryptographic sequence systems synthesis with given correlation properties from 40 to 60 percent with respect to the method of synthesizing a signal system based on the enumeration of all possible sequence variants. When implementing this method, there may be gaps (losses) in finding the best signals in terms of signal correlation properties. But, as studies have shown, the percentage of such losses is insignificant, and for these periods it is no more than 8 percent.

Table 1. Ensemble properties of complex signals various systems

Signal classes	Sequence period	«Dense packing» boundaries	The number of pairs of sequences that satisfy the boundary
M-sequence	31	9	3
Sequences with 3-level CCPF	31	9	495
Cryptographic signals	31	9	1465137
M-sequence	127	27	36
Sequences with 3-level CCPF	127	17	11610
Cryptographic signals	127	23	47 053
M-sequence	255	36	28
Sequences with 3-level CCPF	–	–	–
Cryptographic signals	255	36	17599
M-sequence	511	63	276
Sequences with 3-level CCPF	511	33	147500
Cryptographic signals	511	63	2666671
M-sequence	1023	100	435
Sequences with 3-level CCPF	1023	65	338000
Cryptographic signals	1023	100	5293538

We will evaluate the ensemble properties of this signal system. It should be noted that nonlinear discrete cryptographic signals, in contrast to the known classes of signals used in various ICS applications, can be synthesized for any discrete signal period values. The synthesis of this signal class is based on the limitations associated with the boundary values of the functions of auto - and cross-correlation signals in periodic and aperiodic modes of information transfer. The volume of nonlinear cryptographic signals system (coding power) is determined, firstly, by the requirements resulting from the use of this signal class (detection and measurement of signal parameters, the data transfer mode of users, etc.), and secondly, by the requirements imposed on from the point of view of such indicators of the effectiveness of the functioning of ICS as the noise immunity of signal reception, information secrecy of the system. The user (owner) of the system, on the basis of these restrictions, must make a compromise decision on the choice of an ensemble of non-linear cryptographic signals with the necessary properties.

For most ICS applications, large signal sets with good cross-correlation properties are of interest. That is why the problem of the signal system synthesis was considered as a complex problem, including signal synthesis with the necessary (for certain conditions) ensemble, correlation, and structural properties.

Table 1 shows the data characterizing the ensemble properties of CS in comparison with M-sequences and sequences with 3-level CCPF.

Analysis of the data presented in Table 1 shows that CS have significantly better ensemble properties compared to M - sequences and sequences with 3-level CCPF.

Table 2 shows the data characterizing CS correlation properties for various periods. In particular, the following are given: the dimension (period) of the cryptographic symbol sequence studied; the boundary values of the side peaks of the autocorrelation functions and the signals number satisfying a given boundary in the CS class for various correlation functions; the smallest side peaks of various correlation functions and their number; signal system volume (including the number of CS pairs satisfying boundary values for the corresponding sequence period), etc.

Table 2. Cryptographic discrete signals correlation properties

№		1	2	3	4	5
Segment dimension CS		31	63	127	511	1 023
Uncertainty function boundary values		9	17	23	59	100
ACPF	CSs satisfying boundary	7 743	10 868	3482	3819	8 513
	Min R_{smax}	5	9	17	45	77
	CS with min Rsmax	155	14	51	6	9
ACAF	CSs satisfying boundary	3 622	7 166	1302	1951	6 194
CCPF	Total number of pairs	29 977 024	59 056 712	6 062 162	7 292 380	36 235 584
	Pairs satisfying boundary	1 465 137	12 214 869	47 053	122 835	5 293 538
	Min R_{smax}	5	11	19	51	79
CCAF	Pairs satisfying boundary	14 537 423	54 822 445	1 619 780	3 466 713	35 083 491

Analysis of the data in the table shows the following. So for the sequence period N = 63, the number of cryptographic discrete sequences pairs that satisfy the specified boundary value of the maximum side lobes of the CCPF - 17 is 12 214 869. For linear sequences class representative - sequences with a three-level cross-correlation function (Gold sets, which is optimal from the point of view of the cross-correlation functions of signals [1]), the number of pairs of signals satisfying a given boundary is - 975. The excess of CS over an ensemble composed of M-sequences is more than

10^7. For the sequence period N = 1023, the number of cryptographic discrete sequences pairs that satisfy the set boundary value for the cross-correlation functions side lobes (CCF) – 100, is 5 293 538, whereas for linear sequences class representative M-sequences, the pairs number satisfying a given boundary is - 435, i.e. signal system excess is more than 10^5.

With a slight decrease in the requirements for the limiting value of the maximum lateral peak of the CCF (in fact, reducing the noise immunity of reception), in accordance with which the selection of signals is carried out, the information security performance of the ICS can be significantly improved. So, for the period of the sequence N = 127, increasing the border value by 1.2 dB will allow increasing the ensemble volume with M=11610 (with limit value R_{smax}=17), up to 9 006 648 signals (with limit value R_{smax}=27), i.e. more than 700 times.

Thus, by varying the boundary values of the side-lobe level of the corresponding correlation function (taking into account the requirements for a telecommunications system signal reception noise immunity and systems information security point of view), the tasks of achieving the necessary noise immunity values of signal reception and telecommunications signals information secrecy.

The ICS immunity, and one of its components - the structural secrecy of the system, is largely determined by the structural or statistical properties of the signals - data carriers in the system. Statistical properties studies are carried out in the methodology of statistical tests framework based on statistical tests. In our opinion, the most acceptable (for practical use) testing methods are: FIPS PUB 140-1, AIS 20 и AIS 31, NIST 800-90b, NIST 800-22. In the process of research using the methodology NIST SP 800-22 [10] the implementation of a cryptographic sequence of characters has been tested.

The simulation results showed that nonlinear CS statistical properties (in terms of estimated probabilities values) are within the acceptable values. And this, in turn, means that the CSs satisfy the requirements for pseudo-random sequences: unpredictability of following characters, irreversibility, chance, equiprobability, independence, unpredictability, indistinguishability, etc. Essentially, CSs are indistinguishable from random sequences. Thus, using them as a physical data carrier will increase the structural and information secrecy (cryptographic resistance) of ICS.

5 Derived signal systems synthesis based on cryptographic discrete symbol sequences

Among the systems of phase-shifted signals, many are based on Walsh systems. [1-2]. 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 [11].

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 3 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 3. CS with minimal ACPF side lobes

1	1110001111101000011111011100110011000101000110101101001001100101
2	1000010010000100101110011010000000110010010000010111001110011101
3	0000100100001001011100110100000001100100100000101110011100111011
4	0000100100001001011100110100000001100100100000101110011100111011
5	0001001000010010111001101000000011001001000001011100111001110110
6	0100100001001011100110100000001100100100000101110011100111011000
7	0000100101110011010000000110010010000010111001110011101100010110
8	0001001011100110100000001100100100000101110011100111011000101101
9	0010010111001101000000011001001000001011100111001110110001011010
10	0100101110011010000000110010010000010111001110011101100010110100
11	0000000010100010011000001111100001101101110001101000010111100101
12	0000000101000100110000011111000011011011100011010000101111001010
13	0000001010001001100000111110000110110111000110100001011110010100
14	0100011110001100000100110010000000011011111011100101011000010110

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} do 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 4 shows the results of studies of the correlation functions 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 $\frac{R_{\text{макс}}}{\sqrt{N}}$; expected value of the emission module $\frac{m_{|R|}}{\sqrt{N}}$; the value of the standard deviation of emissions $\frac{D_{(R)}^{1/2}}{\sqrt{N}}$ and emission module - $\frac{D_{|R|}^{1/2}}{\sqrt{N}}$. Calculations were carried out for different values of sequence periods (from 30 to 2052).

Analysis of the data given in table. 4, 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.

Table 4. Statistical characteristics of the correlation functions of various classes of signals

Signal types	Specifications	$\frac{R_{\text{макс}}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D_{\lvert R\rvert}^{1/2}}{\sqrt{N}}$	$\frac{D_{(R)}^{1/2}}{\sqrt{N}}$
Nonlinear characteristic sequences	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
Nonlinear cryptographic characteristic sequences	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-sequences	ACAF	0,7 - 1,25	0,32	0,26	0,41
	ACPF	$1/\sqrt{N}$	$1\sqrt{N}$	0	0
	CCAF	1,4 – 5,0	0,54	0,48	0,73
	CCPF	1,9 – 6,0	0,8	0,62	1

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.

Perform an assessment of ICS security against the imposition of false messages when used as a 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 - 2^m complex signals. Change of compliance is carried out at set time intervals and using a control sequence that meets the requirements of randomness. To provide the necessary noise immunity of signal reception, we will use CS systems that have good correlation properties [1-2,4-5].

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 - 2^m 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:

$$P_{imp./message} = (2^{-k})^n, \qquad (16)$$

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 (CCPFT) and non-linear cryptographic sequences (NLCS). The message dimension is set to n = 32. As the sequence period N were selected: 31, 63, 127, 1023. In the calculations were used data on the ensemble NLCS, are given in table 2.

It must be emphasized that in the calculations $P_{imp./message}$ (for use in the system NLCS), 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 $R_{бок.\ max} \leq 1,5\sqrt{N}$.

Table 5. The message imposing probability values for different discrete signal systems

Sequence period (N)	$P_{imp./message}$ values for systems:		
	M-sequence	Sequences with CCPFT	NLCS
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 can be seen from the data table, the values $P_{imp./message}$ for NLCS 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 $P_{imp./message}$ (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 - 2^m complex signals and apply nonlinear cryptographic signals, provide high levels of system security from unauthorized data modification and the imposition of false information.

In essence, the presented system of providing imitability is [12-13] 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, based on the implementation of the dynamic mode of ICS functioning and using cryptographic discrete signals as information carriers; algorithm for deciding the truth 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.

6 Conclusions

Information exchange methods used in the information and communication system based on a fixed correspondence: message bit (m bit) signal (2^m signals) in the information channel and use (for a long time) in the synchronization channel of the same broadband signal (and the signals used are constructed using linear laws), do not allow to achieve the necessary values of noise immunity and information security of operation ICS. A comprehensive solution to the problem of ensuring noise immunity and information security of ICS operation can be achieved, including, based on the implementation of a dynamic information transmission mode, in which compliance: message bit - the signal changes over time according to the law, which can be predicted with a probability not exceeding the allowable in the system the values and applications of signals with the necessary correlation, ensemble, structural properties. At the same time, signal systems should be based on nonlinear rules for constructing. For the first time, a method for synthesizing nonlinear cryptographic discrete complex signals was obtained, which uses key data as well as random (pseudo-random) processes and allows you to create signals with the necessary ensemble, structural and correlation properties, which makes it possible to improve ICS performance indicators impacts. Improvement of these efficiency indicators is achieved, in particular, due to the possibility of forming, using the obtained CS synthesis method, large discrete sequences ensembles of almost any period with the necessary side lobes of the auto, cross and butt correlation functions (for various ICS applications) in periodic and aperiodic modes of operation, as well as the statistical characteristics of the correlation functions (CF), which are not inferior to those of the best, from the CF point of view, linear classes of signals.

The volume of the system of nonlinear CS (coding power) is determined, firstly, by the requirements resulting from the use of this class of signals (detection and measurement of signal parameters, the mode of data transmission of users, etc.) and, secondly, by the requirements imposed on the system from the point of view ICS performance indicators such as noise immunity of signal reception, information security of the system. The user (owner) of the system, on the basis of these limitations, needs to make compromise decisions on the choice of a particular ensemble of nonlinear CS with the necessary properties. In general, the problem of synthesizing nonlinear discrete complex CSs is formulated and solved, the ensemble correlation properties of which can be selected depending on the requirements for noise immunity and information security of ICS. A method for optimizing the synthesis of complex nonlinear CS based on the use of abbreviated (directional) enumeration based on the application of the «branches and borders» method is proposed.

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 DSS have improved structural and ensemble properties compared with orthogonal signals.

Currently, mathematical model and software have been developed that implements methods for synthesizing and studying the properties of non-linear cryptographic signal systems, which is almost ready for possible use as part of prototypes and elements of modern digital communication tools, and allows: 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.

References

1. Sarwate, D., Pursley, M.: Correction to "Crosscorrelation properties of pseudorandom and related sequences." Proceedings of the IEEE. 68, 1554-1554 (1980).
2. Ipatov, V.: Spread Spectrum and CDMA. John Wiley & Sons, Ltd., Hoboken (2006).
3. Joye, M., Tunstall, M.: Fault Analysis in Cryptography. Springer-Verlag, Heidelberg (2012).
4. Chen, J., Ling, B., Feng, P., Lei, R.: Computer cryptography through performing chaotic modulation on intrinsic mode functions with non-dyadic number of encrypted signals. IET Signal Processing. 13, 7-13 (2019).
5. Kuznetsov, A., Kavun, S., Panchenko, V., Prokopovych-Tkachenko, D., Kurinniy, F., Shoiko, V: Periodic Properties of Cryptographically Strong Pseudorandom Sequences. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129-134 (2018)
6. Gorbenko, I., Zamula, A., Semenko, A., Morozov, V.: Method for synthesis of perfprmed signals systems based on cryptographic discrete sequences of symbols. Telecommunications and Radio Engineering. 76, 1523-1533 (2017).
7. Goubin, L.: Cryptographic hardware and embedded systems. Springer, Berlin (2006).
8. DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm (2014).
9. Land, A., Doig, A.: An Automatic Method of Solving Discrete Programming Problems. Econometrica. 28, 497 (1960).
10. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (2000).
11. Gorbenko, I., Zamula, A., Semenko, A., Morozov, V.: Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes. Telecommunications and Radio Engineering. 76, 1581-1594 (2017).
12. Gorbenko, I., Zamula, A., Morozov, V.: Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts. Telecommunications and Radio Engineering. 76, 1705-1717 (2017).
13. Hameed, A.: High data rate of a novel modulation scheme based on orthogonal chaotic signals. Telecommunications and Radio Engineering. 75, 1657-1663 (2016).