Information and communication systems (ICSs) must comply with increasingly stringent requirements to ensure the reliability and speed of information transmission, noise immunity, information security. This paper reports the methods to synthesize discrete complex cryptographic signals, underlying the construction of which are random (pseudo-random) processes; the methods for synthesizing characteristic discrete complex signals whose construction is based on using the nature of the multiplicative group of a finite field; the results of studying the properties of the specified signal systems. It is shown that the methods built provide a higher synthesis performance than known methods and make it possible to algorithmize the synthesis processes for the construction of software and hardware devices to form such signals. The win in the time when synthesizing nonlinear signals in finite fields using the devised method is, compared to the known method, for the period of 9,972 elements is 1,039.6 times. The proposed method for synthesizing the entire system of such signals, based on decimation operation, outperforms the known method of difference sets in performance. Thus, for a signal period of 2,380 elements, the win in time exceeds 28 times. It has also been shown that the application of such systems of complex signals could improve the efficiency indicators of modern ICSs. Thus, the imitation resistance of the system, when using complex discrete cryptographic signals with a signal period of 1,023 elements, is four orders of magnitude higher than when applying the linear signal classes (for example, M-sequences). For a signal period of 1,023 elements, the win (in terms of structural secrecy) when using the signal systems reported in this work exceeds 300 times at a period of 8,192, compared to the signals of the linear form (M-sequences)

Keywords: noise immunity of reception, noise immunity, secrecy, information security, discrete sequences, signal synthesis

UDC 621.391
DOI: 10.15587/1729-4061.2021.234674

DEVISING METHODS TO SYNTHESIZE DISCRETE COMPLEX SIGNALS WITH REQUIRED PROPERTIES FOR APPLICATION IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

Ivan Gorbenko*
Doctor of Technical Sciences,
Professor, Chief Designer**
Oleksandr Zamula*
Corresponding author
Doctor of Technical Sciences,
Researcher-Consultant**
E-mail: zamylaaa@gmail.com
*V. N. Karazin Kharkiv National University
Svobody sq., 4, Kharkiv, Ukraine, 61022
**JSC «Institute of Information Technologies»
Bakylina str., 12, Kharkiv, Ukraine, 61166

Received date: 16.04.2021
Accepted date: 26.05.2021
Published date: 25.06.2021

***How to Cite**: Gorbenko, I., Zamula, A. (2021). Devising methods to synthesize discrete complex signals with required properties for application in modern information and communication systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 16–26. doi: https://doi.org/10.15587/1729-4061.2021.234674*

1. Introduction

Global trends in growing threats to information and cybersecurity determine the need to devise and implement new models, methods, and technologies for managing telecommunication networks, information security, services, and quality of service. There is a need to build methods of information exchange, methods to synthesize new classes of complex discrete signals-data carriers with the required ensemble, correlation, and structural properties.

Among the main directions of improving the indicators of information security, noise immunity, and secrecy of ICSs, there are areas that are associated with the use of channels with high-frequency redundancy, significant spatial, structural, energy, and time secrecy. To ensure frequency redundancy at the physical level, discrete signals have been widely used, in which the manipulated parameters change at strictly fixed intervals. The law for changing these parameters is set by discrete sequences that fully determine the properties of discrete signals.

The researchers' efforts are aimed at finding signal ensembles whose characteristics are approaching the boundary of "dense packaging" [1]. Such signals have an ideal periodic auto-correlation function (PACF) and a periodic mutual correlation function (PMCF), and have a significant volume.

A widespread criterion for such an approximation is a minimax criterion that focuses on the synthesis of the en-

semble by minimizing the maximum values of side peaks on a set of all unwanted correlations. Works [1, 2] describe the boundaries for the rms and maximum (peak) values for auto- and mutually-correlation functions. Specifically, the fundamentally achievable values of the maximum side peaks of the periodic autocorrelation function $R^a_{\max}$ ("dense packaging" limits) for the assigned period of the sequence N are determined from the following ratio:

$$R^a_{\max} \geq \begin{cases} 0, \text{if } N \equiv 0 (\text{mod } 4); \\ 1, \text{if } N \equiv 1 (\text{mod } 4); \\ 2, \text{if } N \equiv 2 (\text{mod } 4); \\ -1, \text{if } N \equiv 3 (\text{mod } 4). \end{cases}$$

The above limit values establish the criteria for the synthesis of sequence sets (signatures). Ensembles with values corresponding to the specified boundary are optimal and are termed minimax. For an ideal hypothetical ensemble, $R_{\max}$ is zero, and for any real ensemble, the minimum value of the correlation function can serve as an adequate measure of its proximity to the ideal.

The signals-physical data carriers used in ICSs have low structural secrecy and unsatisfactory ensemble characteristics. That does not make it possible to provide the required (especially for critical infrastructure objects) indicators of information security and noise immunity of data transmission within ICS. That is why improving the indicators of noise immunity and information security of ICSs based on the development of theoretical bases, methods, and tools for synthesizing new classes of optimal complex signals with the required ensemble, correlation, and structural properties is an actual task.

2. Literature review and problem statement

Study [1] gives a general description and analysis of the properties of different classes of signals, with the introduced indicators for the effectiveness of the functioning of multiuser communication systems. That makes it possible to comprehensively approach the issues of using certain signal systems to solve the tasks of ensuring the relevant indicators of the effectiveness of the functioning of such systems. Nevertheless, the cited study does not define how the problems of ensuring the necessary indicators of information security and secrecy of the functioning of systems could be solved. The reason for the inability to provide for the necessary (especially for ICSs operating at critical infrastructure facilities) indicators is the classes of broadband signals that are reported in this work. The evolution of views on ensuring the required indicators of the functioning of data transmission systems is described in work [2]. The work presents theoretical bases for the synthesis of a large number of signal systems, including characteristic signals. That makes it possible, when designing data transmission systems, to reasonably make decisions on the use of certain classes of signals as physical data carriers. Despite the obviously correct decision to use the nonlinear signal classes, the cited work does not provide a description of methods that would make it possible to algorithmize the processes of synthesis of signal systems to build modern software and hardware complexes for synthesizing, forming, and processing signals. Paper [3] reports the principles of building telecommunication systems and selecting signals that could be applied to them. That makes it possible to make design decisions on the construction of such systems, to evaluate the performance indicators of such systems, primarily those that are determined by the properties of the signals used in the systems. At the same time, there is no information about the possibility of practical implementation of methods of synthesis of signal systems. Study [4] addresses purely theoretical issues of optimal reception and processing of signals. The approach used in the cited study is focused on the application of information and communication signals, which are based only on the linear laws of construction. This, in turn, does not make it possible to resolve the issues inherent in modern systems for which it is critical to ensure noise immunity and information security. Paper [5] describes the principles of building modern wireless digital communication systems and gives practical recommendations for the use of types of signals (OFDM), methods of encoding, synchronization, data transmission. It has been shown that the introduction of information exchange methods and certain classes of signals could contribute to resolving issues of ensuring information and frequency efficiency, noise immunity of signal reception, the speed of data transmission. At the same time, no solutions are given to solve the problems of ensuring information security (cryptographic stability, imitation protection) at the physical level of a telecommunication network. Work [6] provides an in-depth analysis of the classification and methods of synthesis of a large number of signals. However, there are no specific solutions for the possible practical implementation of these methods and existing restrictions when applying certain signals for many applications of communication systems. Free from these restrictions is work [7]. It shows the possibility of solving the issues of ensuring information security, noise immunity at the level of the source of complex signals. It is shown that the basis for the construction of signals should be nonlinear rules, and data exchange in the system should be based on a dynamic change of conformity: message – complex signal. However, the cited work does not provide practical methods for constructing such signals. Paper [8] describes approaches to determining the requirements for the properties of signals, the use of which in information systems would make it possible to provide the required indicators of protection against influences from intruders. However, the cited paper does not contain a detailed description of the properties of the signals offered and does not give an assessment of the performance indicators of the systems. Study [9] reports the description and characteristics of the block symmetric encryption standard. The encryption algorithm defined by this standard is used in the implementation of the proposed method of synthesis of complex nonlinear discrete cryptographic signals as a source of pseudo-random process. Paper [10] describes the requirements for the initial sequences of cryptographic information conversion algorithms. It is these requirements that are used to formulae requirements in the synthesis of nonlinear signal systems. At the same time, the cited work does not provide methods for the synthesis of signals as a physical data carrier in communication systems. One of the signal classes offered in the work must have properties that are inherent in random sequences of characters. It is [11] that defines the criteria (requirements) for such sequences.

When synthesizing the signals studied in the cited work, it is necessary to use algorithms for block data encryption, as well as take into consideration the requirements for the properties of random sequences of characters. The rules and requirements for such sequences (so-called random lookups) are given in paper [12]. However, this paper does not provide principles, limitations, practical methods for the synthesis of signal systems.

The systematization of the results of the above studies allows us to believe that existing approaches to the use of signals with a linear law of formation do not make it possible to provide the required indicators of noise immunity and information security. This issue can be resolved by devising theoretical bases, practical methods, and software and technical tools to synthesize, form, and process the systems of nonlinear discrete complex signals with the required properties.

3. The aim and objectives of the study

The purpose of this work is to synthesize, based on the devised methods, discrete complex signals with the improved ensemble, correlation, structural properties, which could improve the performance indicators of ICS operation, namely, the performance of signal synthesis, information security, noise immunity (noise immunity of signal reception and secrecy of functioning) of the system.

To accomplish the aim, the following tasks have been set:

– to determine the mathematical dependence of elements and indexes of elements of the simple and extended Galois fields to devise a method of synthesis of complex signals;

– to build models of the structure of complex nonlinear discrete signals in the finite fields and to investigate the structural secrecy, correlation, and ensemble properties of nonlinear discrete characteristic signals for estimating the indicators of noise immunity and information security of ICSs;

– to define conditions for the functions of signal correlation, which are assigned by a set of systems of nonlinear parametric inequalities, and which are used to devise a method for the synthesis of discrete complex cryptographic signals;

– to investigate the properties of the synthesized classes of nonlinear discrete complex cryptographic signals for use in ICSs as a physical carrier of information.

4. The study materials and methods

The essence of our research hypothesis is as follows. Is it possible to devise methods for synthesizing the systems of complex discrete signals with the required (predefined) correlation, ensemble, structural properties, the use of which in modern ICSs could improve the performance indicators of such ICSs?

The following assumptions apply to a given hypothesis:

– methods of signal synthesis should be based on nonlinear rules;

– there should be an opportunity to synthesize signals for any value of the signal period (the natural series of numbers);

– signals must have high structural secrecy (to define the rule of its synthesis, it is necessary to know at least half of the signal symbols);

– there should be a possibility of software and hardware implementation of signal synthesis methods.

Modeling is used as one of the forms of scientific research. The experimental component involves the use of the designed software complex, which implements the functions of signal synthesis, in accordance with the methods proposed in this work (given as a sequence of actions described mathematically, and which make it possible to achieve a certain result), as well as the study into the properties of signals obtained as a result of the synthesis (hereinafter, Complex). The list of main uses of the developed Complex includes:

– the formation of discrete complex signals (CSs);

– the calculation of correlation functions under the periodic and aperiodic modes of operation;

– the calculation of statistical characteristics (mathematical expectation, variance, rms deviation, excess coefficient) of signal correlation functions under the periodic and aperiodic modes;

– the calculation of the largest and smallest values for the side peaks of correlation functions, their number, and the comparison of their values with the optimal boundary for the corresponding correlation function;

– the synthesis of discrete complex signal systems using the decimation process;

– finding the parameters used in the synthesis of signals (the primary element of the field, Euler functions, mutually simple numbers with some given, etc.).

Scientific research at the theoretical level involved the following:

– the generalization of positions from the theory of groups, fields, rings, in order to employ this mathematical apparatus to devise methods for synthesizing the systems of complex signals in finite fields, approaches from the theory of cryptographic protection of information regarding the construction of block symmetric ciphers in the development of methods for synthesizing complex discrete cryptographic signals;

– the comparison of known provisions from the theory of signal systems with the results of our research regarding the synthesis of signal systems and signal properties;

– the mathematical formalization of the representation of the structure of an object to determine the steps of implementation of the devised methods of signal synthesis, which makes it possible to reproduce these methods and obtain the investigated signals.

5. Results of studying the methods of synthesis and properties of nonlinear discrete complex signals

5. 1. Determining the mathematical dependence of elements and indexes of elements of simple and extended Galois fields to build a method of signal synthesis

A series of requirements are put forward to discrete signals: good correlation properties, uniform spectrum, the permissible level of maximum peaks of the auto- and mutually correlated functions, large volume, the existence of duration values for a large number. We have considered *N*-positional codes (characteristic discrete signals, hereinafter referred

to as CDS) with a two-level periodic auto-correlation function (PACF), the construction of which is based on the use of character ψ of the multiplicative group [2] of the field $GF(p^n)$ for $N=4x+2=p^n-1$ and $N=4x=p^n-1$.

It is shown in [2] that the volume of a signal system (M) is equal to the number of classes of non-inverse-isomorphic coefficients, which can be obtained by decomposing a multiplicative group into adjacent classes according to the class of automorphic coefficients; determined as $M=\Psi(N)/2$, where $\Psi(N)$ is the Euler function. It is also known from [2] that the values of the maximum side peaks of the CDS periodic autocorrelation function take the values $R_\mu=\{-2, 2\}$, or $R_\mu=\{0, -4\}$. Analysis shows that CDSs exist for much higher duration values than M-sequences [1, 2]. At the same time, CDSs, as well as M-sequences, are optimal in terms of PACF and are close to optimal in terms of the aperiodic autocorrelation function (AACF).

The method to form CDS [2] with a duration of N, which employs the table of elements and indexes of Galois field elements compiled in the theory of numbers, becomes difficult to implement already at $n\geq 1$ and $N\geq 100$. This is explained primarily by the fact that at the homomorphic mapping of the elements of field a_i onto a set of symbols of discrete sequence when using the complex-significant function $\psi(a_i)=W_i=-e^{\varphi\pi Ui}$, it is necessary to solve on average $N/2$ equations of the following form

$$a_i \equiv \Theta_j^{U_i} \pmod{P}, \quad i=\overline{0, P-1}, \tag{1}$$

where $U_i=\overline{0, P-2}$ is the index of an element from the field $GF(P)$;

$\Theta_j^{U_i}$ is the j-th primary element of the field;

P is the Galois field characteristic.

To solve the equations in form (1), the pre-calculated tables of elements and indexes of Galois field elements are used. The computational complexity of this method of CDS formation is determined from the ratio:

$$t_\Sigma = N\cdot\left(t_m + t_{ad} + 3\cdot t_w + (N-2)\cdot t_r + (N+1)\cdot t_{com}\right), \tag{2}$$

where t_m, t_{ad}, t_w, t_r, t_{com} is the time of multiplication, addition, writing, reading, and comparison operations, respectively.

Our analysis of expression (2) shows that the main time costs in the construction of CDS are related to the terms $N\cdot(N-2)\cdot t_r$ and $N\cdot(N+1)\cdot t_{com}$.

During our study, an improved method of CDS synthesis was devised, which demonstrates a much lower computational complexity compared to the methods considered in [2]. CDS synthesis is based on the use of the smallest (by value) primary element of the field $GF(P)$ and is assigned by statement 1.

Statement 1. Let the character of the multiplicative group of the field be fixed with the following function

$$\psi(a_i) = e^{j\pi U_i}. \tag{3}$$

Then, the mathematical dependence of elements and indexes of elements of a simple Galois field can be described in the following steps.

An array of elements is formed – the numbers A_i, $i=\overline{0, P-2}$ of the $GF(P)$ field:

$$A(i) = \Theta_j^i \pmod{P}. \tag{4}$$

A group of numbers of the field $GF(P)$ is formed, which is shifted by values per unity, according to the following rule:

$$H(i) = A(i)+1, \text{ if } \Theta_j^i + 1 = 0 \pmod{P};$$

$$H(i) = 1, \text{ if } \Theta_j^i + 1 \equiv 0 \pmod{P}. \tag{5}$$

An array of indexes $X(i)$, $i=\overline{0, P-2}$, is formed, the values of which are the corresponding elements of the field indexes i+1, ordered by the content with the address:

$$A(i): X(i) = X\left[A(i)\right]. \tag{6}$$

An array of $J(i)$ indexes is built, the values of which are the indexes of the array $X(i)$, selected at the address $H(i)$; $J(i)=X[H(i)]$, $i=\overline{0, P-2}$.

The nature of the field elements is calculated by the rule given in [2]:

$$\psi(a_i) = \psi\left[J(i)\right] = \begin{cases} 1, \text{if } J(i) \equiv 0 \pmod 2; \\ -1, \text{if } J(i) \equiv 0 \pmod 2. \end{cases} \tag{7}$$

Let $\phi(a_i)$, $i=\overline{1, \ ^n-1}$ be a Galois field $GF(p^n)$ of power n expansion and the polynomial elements whose power does not exceed n, calculated above the field, $GF(p^n)$, $\Phi_k(x)$ and θ_φ – respectively, the k-th primary primitive polynomial and the j-th primary element of the field. The function of the characters of the homomorphic mapping of the elements of the field $GF(p^n)$ onto the field $GF(2)$, fixed by the function $\psi(a_i)=e^{j\pi ui}$, and the polynomial element of the field a_i is determined from the solution to equation $a_i \equiv \theta_j^{u_i} \pmod{\Phi_k(x), P}$, and u_i is the set of index numbers arranged in ascending order.

Find the analytical dependence of elements and indexes of elements for the case of an extended Galois field.

1) An array is formed of the indexes $u_i'=u_i+1$, $i=\overline{0, p^n-2}$, shifted by value, arranged in ascending order, and an array of polynomial elements a_i of the field $GF(p^n)$:

$$A(i) = \theta_j^i \pmod{\Phi_k(x), P}. \tag{8}$$

2) An array of $H(i)$ polynomial elements of the field $GF(p^n)$ is formed, shifted by values per unity relative to the values of the array $A(i)$:

$$H(i) = A(i)+1, \text{ if } \theta_j^i + 1 \neq 0 \pmod{\Phi_k(x), P};$$

$$H(i) = 1, \text{ if } \theta_j^i + 1 \equiv 0 \pmod{\Phi_k(x), P}. \tag{9}$$

3) An array of indexes u_i is written to the array $X(i)$ at the addresses defined by the values of coefficients at the polynomial $H(i)$ in the P calculus system.

4) An array of $J(i)$, $i=\overline{1, p^n-2}$, indexes is formed, the values of which are the u_i indexes, which are read from the array at the addresses that are set by the values of coefficients at the elements-polynomials $H(i)$ in the P calculus system.

5) A two-character symbol is calculated for all values of the array of indexes $J(i)$

$$\psi(a_i) = \psi\left(\theta_j^i + 1\right) = -\psi\left(J(i)\right) = \\ = \begin{cases} 1, \text{if } J = 0 \pmod 2; \\ -1, \text{if } J \neq 0 \pmod 2. \end{cases} \tag{10}$$

As an example, Table 1 gives CDSs with the number of elements 256. The specified signal was obtained by implementing steps (4) to (7) from the devised method of signal synthesis. The Table 1 also shows the values of the maximum side peaks of the periodic autocorrelation function (PACF) for this signal.

Our analysis of data from Table 1 confirms that a given signal class accepts the values of PACF side peaks [2]. Numerical calculations involving computer simulation of expressions (4) to (7) for signals with a length from 16 to 4,000 elements demonstrated that these steps determine the method for synthesizing nonlinear discrete complex signals in finite fields.

Table 1

CDS with the number of elements of 256 with the values for PACF side peaks

Characteristic signal	PACF
[1, 1, 1, 1, −1, 1, 1, −1, −1, −1, −1, −1, −1, 1, −1, 1, 1, −1, 1, 1, −1, 1, 1, 1, −1, 1, −1, 1, −1, 1, −1, 1, −1, −1, 1, 1, 1, 1, 1, 1, 1, 1, −1, 1, 1, −1, −1, 1, −1, −1, −1, −1, 1, 1, 1, 1, −1, −1, −1, −1, −1, −1, 1, 1, 1, 1, −1, 1, 1, 1, 1, 1, −1, 1, −1, 1, 1, 1, 1, −1, −1, −1, −1, −1, −1, 1, −1, −1, −1, −1, −1, −1, 1, −1, 1, 1, −1, −1, −1, 1, 1, 1, 1, −1, −1, −1, 1, −1, −1, −1, 1, 1, 1, −1, −1, 1, 1, 1, 1, −1, 1, −1, −1, 1, 1, −1, 1, 1, 1, −1, −1, 1, −1, 1, −1, −1, 1, 1, 1, −1, 1, −1, −1, 1, −1, −1, −1, −1, −1, −1, 1, −1, −1, 1, −1, 1, −1, −1, 1, −1, −1, −1, −1, −1, 1, 1, 1, 1, 1, 1, −1, −1, −1, 1, 1, −1, 1, −1, 1, −1, −1, 1, −1, 1, −1, 1, 1, 1, −1, −1, 1, −1, 1, −1, 1, 1, 1, −1, 1, −1, −1, 1, 1, 1, 1, 1, 1, −1, 1, −1, 1, −1, −1, 1, 1, 1, 1, −1, 1, −1, 1]	[256, 0, 0, 0, 0, 0, −4, 0, 0, 0, 0, 0, −4, 0, 0, 0, −4, 0, 0, 0, −4, 0, −4, 0, 0, 0, −4, 0, 0, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, 0, 0, 0, 0, −4, 0, −4, 0, 0, 0, 0, 0, 0, 0, 0, −4, 0, 0, 0, −4, 0, 0, −4, 0, −4, 0, −4, 0, 0, 0, 0, 0, −4, 0, −4, 0, −4, 0, 0, 0, −4, 0, 0, 0, 0, 0, 0, 0, −4, 0, 0, 0, −4, 0, −4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, −4, 0, 0, 0, 0, 0, −4, 0, −4, 0, −4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, −4, 0, 0, 0, −4, 0, −4, 0, −4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, −4, 0, −4, 0, 0, 0, −4, 0, 0, 0, 0, 0, 0, 0, 0, −4, 0, −4, 0, 0, 0, −4, 0, −4, 0, −4, 0, 0, 0, 0, 0, −4, 0, −4, 0, −4, 0, 0, 0, −4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, −4, 0, 0, 0, −4, 0, 0, 0, −4, 0, −4, 0, 0, 0, −4, 0, 0, 0, 0, 0, −4, 0, 0, 0, 0, 256]

The computational complexity of the signal synthesis method (construction time t_c) of CDSs, as it follows from statement 1, can be determined from the following expression:

$$\mathrm{t}_c = N\cdot\left(t_m + t_{ad} + t_{com} + 4\cdot t_r + t_w\right) = \\ = N\cdot\left(t_m + t_{ad} + t_{com} + 5\cdot t_r\right). \quad (11)$$

Expression (11) takes into consideration that the time required to perform operations of writing t_w and reading t_r is equal. Our analysis of (11) shows that the time of CDS construction using the proposed method linearly depends on the period of the sequence that is formed, whereas for a known method (expression (2)) the dependence is quadratic.

The gain in the time of CDS synthesis using the devised methods, compared to the known method, is: for the period N=256, 25.5 times; for the period N=9,972, 1,039 times.

We have devised a method for constructing characteristic signals, which demonstrates a lower computational complexity compared to the method based on the use of difference sets [2]. The specified method for constructing the CDS isomorphism system is set by the following statement.

Statement 2. If the sequence $\{W_i\}$, $i=\overline{1,N}$, which is one of the CDS isomorphisms with the number of elements (period) N is subjected to a decimation operation with the decimation coefficient C, where C is a number that is mutually simple with N ($C\in\varphi(N)$), then the resulting sequence $\{v_i\}$ is the isomorphism relative to the sequence $\{w_i\}$.

The decimation procedure means selecting each C-th character of the code and recording the characters obtained in this way so that

$$v_i = \left(w_i + C\right)\bmod N. \quad (13)$$

To prove this statement, it would suffice to show that the characteristic code $\{w_i\}$, built on the basis of difference sets, with an accuracy to a cyclic shift (automorphism) is the sequence $\{v_i\}$.

Example 1: Let Θ=2, N=10. The CDS isomorphism for these parameters is $w_i = \{-1,1,1,1,-1,1,-1,-1,1,-1\}$, and the non-inverse-isomorphic coefficients accept the values T={1, 3, 7, 9}. The characteristic codes, constructed using the method of difference sets (in accordance with the specified coefficients T), take the form

$$w^1_{t=1} = \{-1,1,1,1,-1,1,-1,-1,1,-1\},$$

$$w^2_{t=3} = \{-1,-1,-1,1,1,1,1,-1,-1,1\},$$

$$w^3_{t=7} = \{-1,1,-1,-1,1,1,1,1,-1,-1\},$$

$$w^4_{t=9} = \{-1,-1,1,-1,-1,1,-1,1,1,1\}.$$

The non-inverse and inverse isomorphisms of the characteristic code, which were built based on a decimation method, take the form

$$v^1_{c=1} = \{1,1,1,-1,1,-1,-1,1,-1,-1\},$$

$$v^2_{c=3} = \{1,-1,-1,1,1,1,1,-1,-1,-1\},$$

$$v^3_{c=7} = \{-1,-1,1,1,1,1,-1,-1,1,-1\},$$

$$v^4_{c=9} = \{-1,1,-1,-1,1,-1,1,1,1,-1\}.$$

To form the isomorphism of a characteristic code, it is necessary to implement (in accordance with (13)) N operations over sampling elements at the appropriate decimation coefficient and N addition operations. The time of execution of these operations is denoted, respectively, t_d and t_r. Then the computational complexity of the decimation method can be evaluated using the following expression:

$$T_{dec} = N\left(t_d + t_r\right). \quad (14)$$

Our analysis of operations performed during the implementation of the method of difference sets shows that the computational complexity of the latter T_{ds} is determined from the following ratio:

$$T_{ds} = N\cdot\left(2\cdot t_r + t_{com} + 0{,}5\cdot t_m\right), \quad (15)$$

where t_r, t_{com}, t_m – the time of execution of reading, comparison, multiplication operations, respectively.

The results of computer simulation and the calculations carried out using (14), (15) show that the proposed method significantly exceeds, in terms of performance, the known method of difference sets. Thus, for the signal period of 2,380 elements, the win in time exceeds 28 times.

5. 2. Building a model of the structure of complex nonlinear discrete signals in finite fields and investigating signal properties

It is known that the probability of imposing false messages (signals) by the enemy is determined, among others, by the ensemble properties of the signals used (system volume, the spectrum of values of the signal period for which signals can be synthesized).

Table 2 gives the generalized data on the number of signal length and signal system volume values for *M*-sequences and characteristic discrete signals.

Table 2

Ensemble properties of signal systems

ΔL	Number of values N		System volume	
	CDS	M-sequences	CDS	*M*-sequences
$0–10^2$	30	4	456	8
$0–10^3$	186	9	29,291	79
$0–10^4$	1,269	11	2,152,943	554

Our analysis of the above analytical ratios, as well as data in Table 2, indicates that CDSs are better compared to the widely used *M*-sequences, Legendre sequences, and others.

It is known that the secrecy of ICS functioning largely depends on the complexity of determining by the station the counteraction to the law of discrete signal modulation (the structural secrecy of the signal system used). We shall evaluate the structural secrecy of nonlinear discrete characteristic signals. To this end, we shall state and prove the statements that determine the relationships between the elements of a finite field.

Statement 3. Let $a_1, a_2, \ldots, a_{(P-1)/2}$ be the elements of the field $GF(p^n)$, then the elements of the field $a_{(P-1)/2+1}, a_{(P-1)/2+2}, \ldots, a_{P-1}$ depend on $(P-1)/2$ first elements and are determined from the following expression:

$$a_{(P-1)/2+i} = P - a_i, \quad (16)$$

$$i = \overline{1,(P-1)/2}.$$

We shall illustrate by an example the possibility of constructing $((P-1)/2+i)$ field elements, provided that the first $(P-1)/2$ elements are known.

Let the characteristic of the field be P=13, the primary element of the field is Θ=2.

Record the elements of a given field:

$$a_1 = 2^0 \bmod 13 = 1; \quad a_2 = 2^1 \bmod 13 = 2;$$

$$a_3 = 2^2 \bmod 13 = 4; \quad a_4 = 2^3 \bmod 13 = 8;$$

$$a_5 = 2^4 \bmod 13 = 3; \quad a_6 = 2^5 \bmod 13 = 6;$$

$$a_7 = 2^6 \bmod 13 = 12; \quad a_8 = 2^7 \bmod 13 = 11;$$

$$a_9 = 2^8 \bmod 13 = 9; \quad a_{10} = 2^9 \bmod 13 = 5;$$

$$a_{11} = 2^{10} \bmod 13 = 10; \quad a_{12} = 2^{11} \bmod 13 = 7. \quad (17)$$

Use expression (16) to obtain $((P-1)/2+i)$ elements of the field $\left(i = \overline{1,(P-1)}\right)$:

$$a_7 = a_{(P-1)/2+1} = P - a_1 = 12; \quad a_8 = a_{(P-1)/2+2} = P - a_2 = 11;$$

$$a_9 = a_{(P-1)/2+3} = P - a_3 = 9; \quad a_{10} = a_{(P-1)/2+4} = P - a_4 = 5;$$

$$a_{11} = a_{(P-1)/2+5} = P - a_5 = 10; a_{12} = a_{(P-1)/2+6} = P - a_6 = 7. \quad (18)$$

The comparison of the corresponding elements of the field given in (17) with the field elements (18) shows that these elements are identical. Given the specified property of a Galois field, the nature of the elements of the field or the CDS symbols that are built in the field are likely dependent. This dependence is determined by statement 4.

Statement 4. Let the character of the elements $\psi(a_i)$ of the field (CDS characters in the field $GF(p^n)$ be determined from the following ratio

$$W_i = \psi(a_i) = \exp\leq(j\pi u_i), \quad (19)$$

and the U_i field element indexes are found by solving the following equation

$$a_i = \Theta_l^i + 1 = \Theta_l^{U_i} \pmod P.$$

Then the characters of the field elements $(P-1)/2+1+i$ $\left(i = \overline{1,(P-1)/2-1}\right)$ (sequence symbols) depend on the characters $\left((P-1)/2-i\right)$ of the first elements of the field, and

$$W_{P-i} = (-1)^i W_{i+1}. \quad (20)$$

We shall illustrate that Statement 4 holds using an example.

Let the characteristic of the field $GF(p^n)$) be P=13, and the primary element of the field be Θ=2. The CDS isomorphism in this field is $W = \{-11-111-1111-1-1-1\}$.

We shall establish the dependence of characters (CDS symbols) in the field GF(13). At i=1: $W_2 = -W_2$; i=2: $W_{11} = -W_3$; i=3: $W_{10} = -W_4$; i=4: $W_9 = W_5$; i=5: $W_8 = -W_6$.

The result is the same if one applies (4) to establish the CDS symbol dependence. Using statement 3 makes it possible to determine $((P-1)/2+i)$ CDS symbols $\left(i = \overline{1,(P-1)/2}\right)$ at known first $(P-1)/2$ symbols. In this case, only the first and $((P-1)/2+i)$-th CDS symbols are not defined, but the $((P-1)/2+i)$-th CDS symbol is determined by the encoding rule [2]. For CDS, the number of symbols K accepting "1", is $K=N/2$. This means that the first CDS symbol can be determined if $P-2$ signal symbols are known. It is easy to verify that the statements also hold for the case of the extended Galois field $GF(p^n)$, that is, for the case when $n>1$.

The relationships among the elements and characters of field elements identified and described in statements 3 and 4 make it possible to increase by at least twice the speed of CDS formation devices.

It is known [2] that the statistical characteristics of correlation functions include the mathematical expectation of outliers (m_u); the mathematical expectation of the modules of maximum side outliers $\left(m_{|u_{\text{макс}}|}\right)$; the rms deviation of side outliers $\left(D_u^{1/2}\right)$; the rms deviation of side outlier modules $\left(D_{|u|}^{1/2}\right)$. Using the developed specialized software, we studied the correlation properties of complex nonlinear discrete signals in finite fields. Table 3 summarizes the statistical characteristics of different correlation functions of the most widely used discrete sequences.

Table 3

Statistical characteristics of the correlation functions of signals

Characteristic	$\frac{m_u}{\sqrt{N}}$	$\frac{m_{\lvert u_{макс}\rvert}}{\sqrt{N}}$	$\frac{D^{1/2}_{\lvert u\rvert}}{\sqrt{N}}$	$\frac{D_u}{\sqrt{N}}$
CDS				
AACF	1.1–1.8	0.28	0.32	0.43
PACF	0.1–1.9	0.15	0.02	0.14
AMCF	1.9–3.2	0.54	0.47	0.72
PMCF	2.5–3.6	0.81	0.61	1.01
M-sequences				
AACF	0.7–1.25	0.32	0.26	0.41
PACF	$1/\sqrt{N}$	$1/\sqrt{N}$	0	0
Meander-inverted PACF	1.3–2.3	0.66	0.49	0.82
AMCF	1.4–5.0	0.54	0.48	0.73
PMCF	1.9–6.0	0.80	0.62	1
Butt correlation function	2.0–5.1	0.83	0.62	1
Random sequences				
AACF	1.5–3.1	0.51	0.65	0.70
PACF	2.0–4.0	0.83	0.68	1
AMCF	2.4–4.3	0.54	0.48	0.70
PMCF	2.75–4.5	0.82	0.62	1
M- sequence segments				
AACF	1.45–4.1	0.52	0.90	0.71
PACF	1.6–4.3	0.79	0.58	1
AMCF	1.4–4.3	0.52	0.49	0.72
PMCF	1.6–5.0	0.80	0.60	1

Our analysis of data in Table 3 indicates that the statistical characteristics of the correlation functions of CDSs are not inferior to the similar characteristics of other signals given in this Table.

5. 3. Defining conditions for signal correlation functions assigned by a set of systems of nonlinear parametric inequalities

Based on the study of the algebraic structure of the systems of nonlinear parametric inequalities (SNPE), we have stated and solved in a general form the problem of the synthesis of a new class of complex nonlinear discrete signals – cryptographic signals (CSs). CSs should be understood as a set of sequences (vectors) of characters of a certain alphabet, which have the required (specified) structural, ensemble, and correlation properties.

The synthesis of such signals is based on the use of random or pseudo-random processes, including algorithms for cryptographic information transformation [7–9].

A CS synthesis problem is to be understood as the problem of constructing the subsets of sequences $\left(W_l^q\right)$, $q=\overline{1,N}$, $l=\overline{1,L}$, whose totality forms a system of signals of the alphabet of dimensionality $M_k=N\times L$. Each subset meets the conditions for structural, ensemble, correlation properties, the spatial and time complexity of signal generation. The synthesis of CSs is based on the use and analysis of the periodic and aperiodic correlation functions.

The mathematical model of the process of synthesis of this signal class takes the form given below.

1. Ensuring the conditions for meeting the requirements for the structural and ensemble properties, the possibilities to form a subset of CSs with permissible time and spatial complexity, including using keys.

2. The construction of CSs W^q, whose periodic auto-correlation functions (PACF) satisfy the system of nonlinear parametric inequalities (SNPE):

$$R^q_{a_1}(l)\le\sum_{i=1}^{L}W_i^q\left(W_{i+l}^q\right)^*\le R^q_{a_2}(l),\ \ l=\overline{1,L-1},\ \ q=\overline{1,N}, \qquad (21)$$

where $R^q_{a_1}(l)$ and $R^q_{a_2}(l)$ are the specified values of PACF implementation, and the indexes are calculated by module $(i+1)$ mod L.

At $1=L$ for all $q=\overline{1,N}$ (21) produces a convolution with the value of L

$$\sum_{i=1}^{L}W_i^qW_{i+L}^q=\sum_{i=1}^{L}W_i^qW_i^q=L,\ \ q=\overline{1,N}. \qquad (22)$$

3. The construction of CDS pairs W^q and W^p, whose functions of mutual correlation (MCFs) meet the requirements determined by a set of SNPE (21), and also meet the requirements for the butt functions of mutual correlation (BFMC) of CDS pairs W^q and W^p with butt discrete words W^{qp} and W^{pq}:

$$R^{qp}_{b_{1,1}}(l)\le\sum_{i=0}^{L-K}W_i^q\times\left(W_{i+l}^p\right)^*+$$
$$+\sum_{i=L-K+1}^{L-1}W_i^q\times\left(W_{i-l+K}^p\right)^*\le R^{qp}_{b_{2,1}}(l); \qquad (23)$$

$$R^{qp}_{b_{1,2}}(l)\le\sum_{i=0}^{L-K}W_i^q\times\left(W_{i+l}^q\right)^*+$$
$$+\sum_{i=L-K+1}^{L-1}W_i^q\times\left(W_{i-l+K}^p\right)^*\le R^{qp}_{b_{2,2}}(l); \qquad (24)$$

$$R^{qp}_{b_{1,3}}(l)\le\sum_{i=0}^{L-K}W_i^q\times\left(W_{i+l}^p\right)^*+$$
$$+\sum_{i=L-K+1}^{L-1}W_i^q\times\left(W_{i-l+K}^q\right)^*\le R^{qp}_{b_{2,3}}(l); \qquad (25)$$

$$R^{qp}_{b_{1,4}}(l)\le\sum_{i=0}^{L-K}W_i^p\times\left(W_{i+l}^p\right)^*+$$
$$+\sum_{i=L-K+1}^{L-1}W_i^p\times\left(W_{i-l+K}^q\right)^*\le R^{qp}_{b_{2,4}}(l); \qquad (26)$$

$$R^{qp}_{b_{1,5}}(l)\le\sum_{i=0}^{L-K}W_i^p\times\left(W_{i+l}^q\right)^*+$$
$$+\sum_{i=L-K+1}^{L-1}W_i^p\times\left(W_{i-l+K}^p\right)^*\le R^{qp}_{b_{2,5}}(l); \qquad (27)$$

and $l=\overline{1,L-1}$ for any combinations of q and p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q\ne p$, where $R^{qp}_{b_{1,j}}(l)$ and $R^{qp}_{b_{2,j}}(l)$, set the (necessary) implementations of PMCF and BFMC, respectively, $j=\overline{1,5}$.

In the systems of nonlinear parametric inequalities (21) to (24) W_i^q and W_i^p are the unknown values of random or pseudo-random CDS symbols W^q and W^p, $q=\overline{1,N}$, to be determined in the process of their construction. Hereafter, systems (21) to (27) are referred to as a model of the subset (vocabulary) of CS.

We shall analyze the systems of nonlinear parametric square inequalities (hereinafter, systems) (21) to (27), using the model introduced.

Systems (24), (25) at 1=L for all $q=\overline{1,N}$ must yield the full convolution with a value of L, that is,

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, \quad q=\overline{1,N}, \tag{28}$$

and (25) produces

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^p = \sum_{i=1}^{L} W_i^p W_i^p = L, \quad p=\overline{1,N}. \tag{29}$$

Systems (23), (25), and (27) at 1=L for all pairs W^q and W^p give the value of the mutual correlation function at a zero offset value in the following form, respectively:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), \quad q,p=\overline{1,N}, \tag{30}$$

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^p = \sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), \quad q,p=\overline{1,N}, \tag{31}$$

$$\sum_{i=1}^{L} W_i^p W_{i+L}{}^q = \sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), \quad p,q=\overline{1,N}. \tag{32}$$

We shall analyze systems (21), (22) for the existence of solutions and independence. Directly from (21), we obtain that for each q of CS W^q there are L unknowns $W_1^q, W_2^q, ..., W_L^q$. To find them, according to (21), one can build a system of L–1 independent SNPE. Further, using (22), we obtain another expression but an equation, in this case. The peculiarity of system (21) is that this system produces a convolution of each q of CSs with a value L. Based on (21), (22), when constructing each of the N subset of CS, one can build N independent SNPE, each of which would contain L–1 quadratic inequalities in the form of (21) and a formally one equation, so that all of them will equal L.

For N=2, SNPEs (28), (29) includes some loss non-linear quadratic equations. Equation (22) is the same as (28), (29), so the last two are already included in system (24), are dependent, so cannot be used. Further, equations (30), (32) coincide, and equation (28) is symmetrical in terms of the correlation function, in relation to equations (30), (31). Therefore, for each pair p and q, the independent is (30).

Based on a detailed analysis, we have that all (23) to (27) SNPEs define different implementations of PMCF and BFMC of only two CSs – W^q and W^p. Therefore, the mathematical model of building two CS W^q and W^p is uniquely defined by five SNPEs in the form of (23) to (27), and, as has already been substantiated, by equation (30).

The above results of our analysis make it possible to determine the complexity of the model and, on its basis, the complexity of building a subset of N CS. When building one CS, it is necessary, depending on the permissible values $R_{a_1}^q(l)$ and $R_{a_2}^q(l)$, determined by the boundaries of dense packing, to consider $\upsilon \geq k$ systems in the form of (22). When building two CS, it is necessary to consider $\upsilon_2 \geq k_2$ systems in the form of (23) to (27), where K_2 is determined by $R_{b_{1,j}}^{qp}(l)$ and $R_{b_{2,j}}^{qp}(l)$. When building N CS, it is necessary to consider $\upsilon \geq K \cdot N$ systems in the form of (30) to (32), where $K{\cdot}N$ is determined by $R_{a_1}^q(l)$ and $R_{a_2}^q(l)$ and $R_{b_{1,j}}^{qp}(l)$ and $R_{b_{2,j}}^{qp}(l)$ acceptable values.

Thus, taking into consideration the boundaries of the physical packing of the CS subset [4], there are opportunities to build the subsets of CS according to (22) and (30) to (32). Similarly, (21), (23) to (27) assign the model of a subset (vocabulary) of CS through the aperiodic auto-correlation functions (AACF). In this case, simplifications are possible. Thus, system (21) ca be represented by analogy in the form of SNPE based on the aperiodic correlation functions, that is,

$$r_{a_1}^q(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{a_2}^q(l), \quad l=\overline{1,L}, \quad m=\overline{1,L}, \tag{33}$$

where $r_{a_1}^q(l)$ and $r_{a_2}^q(l)$ are the assigned, but permissible implementations in terms of "dense packing".

Next, systems (21) to (27) can also be given through the aperiodic mutual correlation functions (AMCF) in the form of a system of nonlinear parametric inequalities

$$r_{b_{1,1}}^{qp}(l) \leq \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r_{b_{1,2}}^{qp}(l); \tag{34}$$

$$l=\overline{1,L}, \quad m=\overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \leq \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \leq r_{b_{2,2}}^{pq}(l); \tag{35}$$

$$l=\overline{1,L}, \quad m=\overline{1,L},$$

where $r_{b_{1,1}}^{qp}$, $r_{b_{1,2}}^{qp}$, $r_{b_{2,1}}^{qp}$, $r_{b_{2,2}}^{qp}$, are the permissible, from the point of view of "dense packing", values of AACF and AMCF.

Taking into consideration the need to ensure cryptographic stability and structural secrecy of pairs or subsets of CS, algorithms of block symmetric transformation or other sources of random or pseudo-random sequences can be used as a source of discrete sequences.

Taking formulas (21) to (27) into account, we defined the steps for the method of the synthesis of discrete complex cryptographic signals:

1. Form random or pseudo-random discrete sequences.
2. Assess the statistical properties of potential CS.
3. Build the required number of potential CS W^q according to system (21) and key data.
4. Find the pairs or subsets of CS W^q and W^p that meet requirements (23) to (27) using the method of "branch and bound"
5. Construct a matrix of states of mutual-correlation functions of all possible pairs of potential CS, which were selected based on the results of the previous step and have all the necessary properties.
6. Analyze the matrix of states and form the required number of subsets or pairs of CS according to (21), (23) to (27); select to a subset only those that meet the requirements.

5. 4. Studying the properties of the synthesized classes of nonlinear discrete complex cryptographic signals

For a series of ICS applications, signals with high structural secrecy, the necessary correlation properties, and a significant volume (ensemble) are required. We shall evaluate the ensemble, correlation, and structural properties of a given signal system.

It should be noted that CS, unlike the known classes of signals used in various ICS applications, can be synthe-

sized for any values of the period of discrete signals. The volume of the system of nonlinear CS is determined by the requirements for the system, in terms of such indicators of the effectiveness of the functioning of the ICS as the noise immunity of reception, secrecy, and information security of the system. Users (owners) of the system, based on these restrictions, need to make compromise decisions on the choice of an ensemble of nonlinear CS with the required properties.

Table 4 gives data characterizing the correlation and ensemble properties of CS of different periods. Specifically, the period of CS; the limit values of side peaks of auto-correlation functions; and the number of signals that correspond to the limit values in the CS class; the smallest values of side peaks of different correlation functions, and their quantity.

Our analysis of the data given in Table 4 indicates that the values of maximum side outliers, the statistical characteristics of CS are not inferior to the corresponding characteristics of signals that are built using *M*-sequences. Thus, for the sequence period of 1,023 elements, the number of CS pairs, satisfying the limit value for the side petals of MCF of 100, is 5,293,538. For *M*-sequences, the number of pairs corresponding to this limit is 435, that is, the excess volume of the CS system is more than 10^4 times. Varying the boundary values of the level of the side petals of the corresponding correlation function, the task of achieving the necessary values of indicators of interference with the resistance of signal reception, interference and information security of the system can be solved.

Table 4

Correlation and ensemble properties of CS

No.	CS segment dimensionality	Uncertain function limit value	PACF			AACF	PMCF			AMCF
			The number of CS that meets the limit	Lowest value u_{max}	The number of CS with the lowest u_{max}	The number of CS that meets the limit	Total number of pairs	The number of CS that meets the limit	Lowest value u_{max}	The number of CS that meets the limit
1	31	9	7,743	5	155	3,622	29,977,024	1,465, 137	5	14,537, 423
2	63	17	10,868	9	14	7166	59,056,712	12,214, 869	11	54,822, 445
3	127	23	3,482	17	51	1,302	6,062,162	47,053	19	1,619, 780
4	511	59	3,819	45	6	1,951	7,292,380	122,835	51	3,466, 713
5	1,023	100	8,513	77	9	6,194	36,235,584	5,293, 538	79	35,083, 491

To study the structural properties of CS, the procedures for testing the generators of random (pseudo-random) sequences, which are defined in [10, 11], are used. The test results showed that the CSs meet the requirements for random sequences [12]: the unpredictability of symbols, irreversibility, randomness, equal probability, independence, etc. Thus, the structural properties of CS do not differ from the properties of random sequences.

6. Discussion of results of studying the methods of synthesis of discrete complex signals for use in modern information and communication systems

Our results indicate that the proposed methods to synthesize characteristic discrete signals (CDS) in finite fields can significantly increase the efficiency of the synthesis of these signals. Indeed, the winning time for the synthesis of nonlinear signals in finite fields using the devised method (statement 1), compared to the known method, for the CDS period of 256 elements, is 25.5 times, and for the period of 9,972–1,039.6 times. The method to synthesize the entire CDS system based on the decimation procedure (statement 2) was built. The results of computer simulation and the calculations carried out using (14), (15) show that the proposed method of synthesis based on a decimation operation surpasses a known method of difference sets in terms of performance. Thus, for the signal period of 2,380 elements, the win in time exceeds 28 times. The relationships among the elements and the characters of field elements identified and described in statements 3 and 4 make it possible to increase by at least twice the speed of CDS formation devices. Our study into the correlation properties of CDS has shown that the values of maximum side peaks, as well as statistical characteristics of various correlation functions (Table 1), are not inferior to similar characteristics of the noise immunity best-known linear signals. This, in turn, means that the indicators of noise immunity when receiving the signals offered will be no worse than when using known signal systems. At the same time, the structural properties of CDS, which are associated with the complexity of determining by the station of counteraction to the law of signal formation, have been significantly improved compared to known signal systems. That directly follows from statement 4. It should be noted that the use of these signals makes it possible to improve the indicators of information security, namely the probability of the enemy imposing false messages (signals). It is known that this indicator is determined, among other things, by the ensemble properties of the signals used (system volume, the spectrum of values of the signal period for which signals can be synthesized). Our analysis of the above analytical ratios, as well as data in Table 1, indicate that CDS, in terms of ensemble properties, are better compared to a series of sequences used, such as *M*-sequences, Legendre sequences, and others.

By studying the algebraic structure of the systems of nonlinear parametric inequalities, as well as by analyzing the periodic and aperiodic functions of correlation, we have built a mathematical model of the process of synthesis of discrete complex signals (21) to (27), as well as practical methods for synthesizing the nonlinear discrete complex cryptographic signals (hereinafter, CS). The synthesis of CS employs random or pseudo-random processes (including cryptographic algorithms), which makes it possible to create the sequences of symbols (signals) of a certain alphabet. Such sequences satisfy the requirements of irreversibility, randomness, unpredictability, and possess the required structural, ensemble, and correlation properties, as evidenced by the data given in Table 4.

The results reported here suggest that the use of CS leads to improved indicators of noise immunity, information security, the secrecy of information and communication systems, noise immunity of signal reception under the influence of various types of interferences. The applied software complex, the peculiarities of which are modularity and flexibility, the use of a single web service for the simultaneous use of the capabilities of the complex by many users, allowed us to implement the functions of synthesis, formation, processing, and studying signal properties. This indicates the possibility of introducing the obtained results into acting and promising software and hardware tools at the physical level of information and communication systems.

Our study considers the processes of synthesis, formation, processing of two classes of discrete complex signals, namely, cryptographic signals and signals in finite fields. The software means that implement the functions of synthesis, formation, processing and studying the properties of these signal systems are almost ready for possible use as part of prototypes and elements of digital communication means for modern ICS. The possibilities of using the devised methods for synthesizing the specified signal classes in modern communication systems can be limited only by the characteristics of the used hardware tools and the peculiarities of the implementation of the software complex (programming language, principles of interface construction, etc.).

Further development of this research may include the development of methods to synthesize and investigate the properties of discrete complex signal systems, which are formed by the symbol-wise multiplication of the so-called output signals and producing signals. Moreover, it is proposed to use orthogonal discrete signals as output signals, and discrete complex cryptographic signals, and discrete complex signals in finite fields as producing signals. In this sense, the results of our study reported here could prove useful. There is reason to believe that the signals received in this way would demonstrate improved ensemble, correlation, and structural properties, which could allow them to be used as a physical data carrier in the ICS, for which the requirements of information security and noise immunity are critical.

7. Conclusions

1. Based on the established mathematical dependence of the elements and indexes of elements of the simple and extended Galois fields, we have devised methods for synthesizing the nonlinear complex characteristic discrete signals (CDS) in finite simple and extended fields. These methods make it possible to significantly increase the speed of signal synthesis. That has been confirmed by the results of numerical modeling. The modeling showed that the win in the synthesis time of a separate CDS using the devised method, compared to the known method, for the number of elements of 256, is 25.5 times, and for the number of elements of 9,972–1,039.6 times. As regards the resulting method for synthesizing the entire signal system based on a decimation method, the win in the time of synthesis is (with the number of signal elements of 2,380) exceeds 28 times.

2. To assess the indicators of noise immunity and information security of the functioning of information and communication systems (ICS), an effective tool is to study the properties of signals-physical data carriers in such systems. The model of the structure of complex nonlinear discrete signals in finite fields, as well as the ensemble, statistical, and correlation properties of such signals, determined during our research, suggest that these indicators of ICS are significantly improved. Thus, for a signal period of 1,023 elements, the win, in terms of structural secrecy, when using CDS, relative to the use of linear signals, is 50 times, and for the number of elements of 8,192 more than 300 times. For the duration of CDS of 256 elements, the win, compared to the use of linear *M*-sequences, is 3 dB. Since the indicators of information security, namely, the likelihood of the enemy imposing false messages, depend on the ensemble characteristics of the signals, the improved ensemble properties of nonlinear CDSs can significantly improve this indicator of the efficiency of the system.

3. We have defined the conditions for the functions of signal correlation, which are assigned by a set of the systems of nonlinear parametric inequalities, which has made it possible to devise a method for the synthesis of discrete complex cryptographic signals. Distinctive features of this approach in the development of theoretical bases and methods of synthesis are the use of random (pseudo-random) processes, the ability to reproduce signals in space and time using the parameters applied in their synthesis, including cryptographic keys. These features of the approach to signal synthesis make it possible to form signals that are nonlinear according to the law of their creation since they use random (pseudo-random processes). In addition, such signals can be synthesized for any period (an even or odd number of elements).

4. The resulting class of nonlinear CS, as shown by our study using methods of computer simulation, possesses improved, compared to known linear classes of signals, structural, ensemble, and correlation properties. Such signals (sequences) satisfy the requirements for irreversibility, randomness, unpredictability, that is, they do not differ from random sequences. That makes it possible to improve the secrecy and information security of the system. Thus, for a sequence period of 1,023 elements, the volume of the CS system is more than 15 times higher than the volume of the signal system with a 3-level function of mutual correlation, and is more than 1,200 times higher than the volume of the system made up of *M*-sequences. Given the improved ensemble properties of the CS and a dynamic change in the match between a bit of the message and a complex signal, it is possible to improve the indicators of information security. Thus, the imitation resistance of the system (the probability of imposing false messages) when using CS with a signal period of 1,023 elements is four orders of magnitude higher than when using linear signal classes (for example, *M*-sequences).

Acknowledgments

The staff at the Department of Information Systems and Technologies Security, Kharkiv National University named after VN Karazin, E.S. Semenko, Ho Tri Luc made a certain contribution to this research. We thank the management of AT "Institute of Information Technologies" for financial support in preparing the manuscript for publication.

References

1. Varakin, L. E. (1985). Sistemy svyazi s shumopodobnymi signalami. Moscow: Radio i svyaz', 384.
2. Sverdlik, M. B. (1975). Optimal'nye diskretnye signaly. Moscow: Radio i svyaz', 200.
3. Liang, Q., Liu, X., Na, Z., Wang, W., Mu, J., Zhang, B (2018). Communications, Signal Processing, and Systems. Proceedings of the CSPS Volume III: Systems. Springer, 1219. doi: https://doi.org/10.1007/978-981-13-6508-9
4. Ipatov, V. P. (2005). Spread Spectrum and CDMA. Principles and Applications. John Wiley & Sons Ltd. doi: https://doi.org/10.1002/0470091800
5. Michael Yang, S.-M. (2019). Modern Digital Radio Communication Signals and Systems. Springer, 664. doi: https://doi.org/10.1007/978-3-319-71568-1
6. Gantmaher, V. E., Bystrov, N. E., Chebotarev, D. V. (2005). SHumopodobnye signaly. Analiz, sintez, obrabotka. Sankt-Peterburg: Nauka i Tekhnika, 400.
7. Gorbenko, I. D., Zamula, A. A., Morozov, V. L. (2017). Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts. Telecommunications and Radio Engineering, 76 (19), 1705–1717. doi: https://doi.org/10.1615/telecomradeng.v76.i19.30
8. Gorbenko, I. D., Zamula, A. A. (2017). Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems. Telecommunications and Radio Engineering, 76 (12), 1079–1100. doi: https://doi.org/10.1615/telecomradeng.v76.i12.50
9. DSTU 7624:2014. Informatsiyni tekhnolohiyi. Kryptohrafichnyi zakhyst informatsiyi. Alhorytm symetrychnoho blokovoho peretvorennia (2015). Kyiv: Minekonomrozvytku Ukrainy.
10. Kuznetsov, A. A., Moskovchenko, I. V., Prokopovych-Tkachenko, D. I., Kuznetsova, T. Y. (2019). Heuristic methods of gradient search for the cryptographic boolean functions. Telecommunications and Radio Engineering, 78(10), 879–899. doi: https://doi.org/10.1615/telecomradeng.v78.i10.40
11. NIST 800-90 b. Recommendation for the Entropy Sources Used for Random Bit Generation (2012).
12. Tesa , P. (2017). Influence of Non-Linearity on Selected Cryptographic Criteria of 8x8 S-Boxes. Acta Informatica Pragensia, 6 (2), 162–173. doi: https://doi.org/10.18267/j.aip.107