Cybernetics and Systems Analysis, Vol. 46, No. 3, 2010

WORKS OF THE KIEV SCHOOL OF THEORETICAL CRYPTOGRAPHY

M. N. Savchuk

UDC 681.3.06:519.248.681

Abstract. *This paper presents works of the Kiev school of theoretical cryptography that are carried out mainly during the last two decades in the fields of cryptographic methods of information security, cryptanalysis, and related mathematical disciplines.*

Keywords: *cryptography, cryptanalysis, probabilistic combinatorics, probability on algebraic structures, random placement, statistical criterion, estimate of complexity of cryptalgorithms, asymptotic analysis.*

INTRODUCTION

A vital part of an information security system consists of cryptographic mechanisms. Academician B. E. Paton, President of NAS of Ukraine, and Academician V. M. Glushkov, the founding director of the Cybernetics Institute of AS of UkrSSR, realized the necessity of development of cryptological investigations as long ago as at the beginning of the 70s of the last century.

By the end of the 40s of the last century, the main attention in the Soviet Union was given to the creation of merely technical means of enciphering. It became obvious at the interface of the 40–50s that a reliable protection of state secrets is impossible without a serious mathematical substantiation. To improve the cryptographic service, a group of leading mathematicians was recruited. The organizer and research supervisor of studies of this service was Vladimir Yakovlevich Kozlov, an outstanding mathematician and a Corresponding Member of the Russian Academy of Sciences and an Academician of the Academy of Cryptography of the Russian Federation later on.

On the initiative of V. Ya. Kozlov, a research division for carrying out cryptological investigations was created in the Cybernetics Institute of AS of UkrSSR in 1973. Beginning with its creation, this division was headed by Academician I. N. Kovalenko (together with A. M. Fal' from the middle of the 80s). The division was engaged in the solution of mathematical problems conditioned by interests of cryptography. Problems were formulated by leading experts of the cryptographic service who worked in Moscow. The division successfully worked till 1992.

In the independent Ukraine, active investigations in the field of cryptography were continued in the Cybernetics Institute. The results obtained and also investigations on reliability theory were highly prized. In 2001, the State Prize for a cycle of works on safety and reliability of information technologies in the field of science and engineering was awarded to a scientific collective that mainly consisted of specialists of the Cybernetics Institute. Moreover, the State Prizes in the field of science and engineering were awarded in 2004 and 2009 to scientific collectives including specialists in the field of cryptography and steganography.

Cryptological investigations in establishments of NAS of Ukraine are greatly supported by Academician I. V. Sergienko, the director of the V. M. Glushkov Cybernetics Institute. On his initiative, a session of the Presidium of

Physicotechnical Institute of the National Technical University of Ukraine "Kiev Polytechnic Institute," Kiev, Ukraine, *msavchuk@ukrpost.net.* Translated from Kibernetika i Sistemnyi Analiz, No. 3, pp. 52–68, May–June 2010. Original article submitted February 17, 2010.

NAS of Ukraine was held in 2001, which was devoted to problems of information security and development of cryptological investigations. At this session, a report of I. N. Kovalenko was presented.

At the Information Security Faculty created in the Physicotechnical Institute of NTUU "KPI" in 2000, the Department of Mathematical Methods of Information Protection was created under the guidance of M. N. Savchuk, doctor of physical and mathematical sciences and a disciple of Academician I. N. Kovalenko. Present and former employees of the Cybernetics Institute were involved in the teaching of special disciplines at the Department.

Based on this Department, according to the resolution of the Presidium of NAS of Ukraine, the scientific seminar "Problems of Modern Cryptology" was initiated in 2001 and functions on a regular basis. At this seminar, the subjects of reports are very diverse and cover various aspects of synthesis and analysis of cryptographic systems of information protection and mathematical problems of theoretical cryptography. We point out some of them.

– Construction of algebraic models of symmetric cryptosystems.

– Analysis of cryptoresistance of enciphering algorithms.

– Investigations of problems of probabilistic combinatorics and their use in cryptography.

– Invariance theory and methods of solution of systems of linear equations over finite fields and rings.

– Methods of solution of systems of linear Boolean equations with corruptions and also systems of random pseudo-Boolean equations.

– Methods of solution of systems of nonlinear Boolean equations.

– Spectral methods in steganography.

– Information protection schemes in dynamic environments.

– Algorithms of realization of operations in a group of points of an elliptic curve.

– Comparative analysis of standards of digital signatures in Ukraine and Russia that are based on elliptic curves.

– Probabilistic methods of testing polynomials for irreducibility.

– Investigation of methods for testing generators of random sequences.

– Secret sharing schemes.

– Key distribution methods.

– Creation of hardware-software systems of multiple-precision arithmetic and their use in cryptography.

– Algebraic attacks on stream ciphers.

– Selection criteria and an algorithm of generating long-term keys for GOST 28147–89.

– Propositions concerning the creation of new block symmetric enciphering algorithms with a view to implementing them in Ukraine.

– Efficient algorithms of quantum computations and their application in cryptography.

– Investigation of new methods of construction of one-sided functions.

(The list of reports of the seminar "Problems of Modern Cryptology" that were presented and discussed in 2001–2009 is given at the end of this article.)

One of the most important lines of investigations connected with mathematical problems of cryptographic protection of information is the probabilistic-combinatory approach with application of methods of abstract algebra, complexity theory, and asymptotic analysis. The use of well-developed analytical methods and limit theorems of probability theory allows one to better investigate the dynamics of development of complex systems in practical and theoretical aspects. The probabilistic approach to combinatorial problems in set-theoretic statements allows one to achieve greater clearness, to consider many different classes of problems from a unified viewpoint, and to solve them by unified methods. Among various areas of probabilistic combinatorics, we will single out several lines of investigation.

– Probabilities on algebraic structures. Invariance theory.

– Coding theory.

– Random placements and their use in cryptology.

- Random reflections, substitutions, and graphs.
- Order statistics, extreme values, and optimization.
- Combinatorial methods in the theory of random processes.
- Statistical criteria and their use in cryptology.
- Algebraic and combinatorial models of symmetric cryptosystems.
- Combinatorially random algorithms and their use in cryptology.
- Statistical and algebraic methods in cryptanalysis.
- Algebraic-probabilistic approaches in the analysis of asymmetric cryptosystems.
- Classical and postquantum models of computations.

In these directions, investigations were carried out by specialists of various mathematical schools including specialists of the Kiev school of theoretical cryptography. Let us give a brief review of some works of this school (mainly for the last 10–20 years).

PROBABILITIES ON FINITE ALGEBRAIC STRUCTURES

Algorithms of decoding corrupted linear codes over the field $GF(2)$. As is well known, the decoding of linear codes of general form is an *NP*-complete problem. The search for decoding algorithms that have a smaller complexity in comparison with the method of maximum likelihood and are efficient in practical applications is of significant interest, in particular, for methods of information protection and cryptanalysis. In cryptanalysis, the cases of strongly corrupted linear codes of large length when the probability of correct transmission of a symbol is close to 1/2 are of the greatest interest. In another interpretation, these algorithms are also used for the solution of systems of linear equations with corrupted right sides in Galois fields. Efficient methods for the solution of systems of linear equations with corrupted right sides over finite fields, rings, and groups form a powerful apparatus in cryptanalysis. The algorithm proposed in [1] considerably reduces the amount of computations in decoding and solving systems of linear equations and is a new step in this field. The main result of [1] is as follows.

Let a linear code over the field $CF(2)$ be specified by a generator matrix $A=(a_{ij})$, $i=\overline{1,N}$, $j=\overline{1,n}$, with the help of which an information word $\bar{x}=(x_1, x_2, \dots, x_n)$ is encoded into a codeword $\bar{y}=(y_1, \dots, y_N)$. This codeword is transmitted along a binary symmetric channel with the probability of correct transmission of the *i*th symbol p_i. Under definite asymptotic (as $n\to\infty$) conditions imposed on the distribution of (not necessarily independent) elements of the random matrix *A*, on the probability of correct transmission of p_i, and on the number of equations, there is a decoding algorithm having an asymptotically average complexity $L\le\exp\{Cn(1+\varepsilon)\log^{-1}n\}$, $C=\text{const}>0$. The algorithm is based on the stage-by-stage summation of rows of the submatrices formed after partitioning the extended matrix $\overline{A}$ (with the addition of a received word in the capacity of the $(n+1)$th column to the matrix *A*), the subsequent sorting of each matrix obtained in this way, new summation, and the repetition of this procedure before obtaining several equations with one unknown. Parameters matched in a special way at each stage of the algorithm make it possible to reduce its decoding complexity to the subexponential complexity.

Algorithms for decoding corrupted linear codes based on the sorting and summation of rows of generator matrices are proposed in [2, 3]. Algorithms of decoding such a linear code are constructed that reconstruct an information word $\bar{x}=(x_1, x_2, \dots, x_n)$ from a received word $\bar{y}=(y_1, \dots, y_{N_0})$ and a generator matrix unknown in advance and that are based on the summation of rows of the extended matrix $\overline{A}$ formed by the addition of a received word to the generator matrix in the capacity of its last column.

The described algorithms are used for decoding a series of linear codes *M* over $GF(2)$ with one generator matrix for all codes of the series and different information words that are transformed into codewords and are transmitted along a binary symmetric memoryless channel with the probability of correct transmission p_i^l, $l=\overline{1,M}$, $i=\overline{1,N_0}$, dependent on the numbers of a code and a symbol.

For these methods, an asymptotic analysis is performed and asymptotic estimates of complexity of algorithms are found for elements of the generator matrix that are independent in the aggregate when $\mathbf{P}\{a_{ij} = 1\} = 1 - \mathbf{P}\{a_{ij} = 0\} = \rho \leq 1/2$, $i = \overline{1, N_0}$, $j = \overline{1, n}$, and corruptions are strong, i.e., for N_0, as $n \to \infty$, $p_i \to 1/2$ and $p_i^l \to 1/2$, $i = \overline{1, N_0}$, $l = \overline{1, M}$. The algorithms described are especially efficient for sparse generator matrices and codeword dimensions insufficient for other methods.

The considered algorithms can be used for estimating the cryptographic resistance of information protection systems, in cracking them with the help of cryptographic analysis, and also in investigating properties and parameters of random systems of equations with corruptions over finite algebraic structures (groups, rings, and Galois fields) and in developing methods for their solution.

Experimental investigations of decoding algorithms. In [4], the following two methods of decoding linear codes described above are considered: the maximum likelihood method and Monte Carlo method. The algorithm of maximum likelihood consists of an exhaustive search for all 2^n information words $X^{(k)}$, $k = \overline{1, 2^n}$, for each of which we find the Hamming distance $\rho_k = |AX^{(k)} - \widetilde{Y}|$, $k = \overline{1, 2^n}$, between the code $AX^{(k)}$ and received $\widetilde{Y}$ words. The word that corresponds to the minimal value of ρ_k is the sought-for word. If a minimum attained on several vectors, then an unambiguous reconstruction of an information word with a given probability of error and the code length N is impossible.

The Monte Carlo method of decoding a code consists of searching for a randomly uncorrupted system of n equations of n variables among the equations specifying the code in the solution of this system in the case when the determinant of the system is not equal to zero and checking the obtained solution X^* using a randomly chosen (N', n) submatrix A^* with the corresponding symbols of the received word $\widetilde{Y}^*$. If the Hamming distance $\rho^* = |A^* X^* - \widetilde{Y}^*|$ does not exceed some given threshold C, then X^* is considered to be the decoded information word. In cases when the determinant is equal to zero or $\rho^* > C$, we pass to the search for a new system of n equations.

In [4], the results of an experimental investigation of the two mentioned algorithms are presented for finite values of the parameters n, N, and Δ, the reliability and laboriousness of these algorithms are compared, and also their experimentally obtained characteristics are compared with asymptotic theoretical values.

Systems of linear equations with corrupted right sides over rings. A. N. Alekseychuk and S. M. Ignatenko [5–7] investigated systems of linear equations with corrupted right sides over a residue ring modulo 2^N. Such systems of equations are classical objects of investigations in cryptography and, as a rule, are used in constructing correlation attacks on symmetric cryptosystems (generators of pseudorandom sequences and block and stream ciphers). In connection with the development of synthesis methods and extension of the sphere of application of nonbinary software-oriented stream ciphers, a heightened interest of specialists in systems of equations with corrupted right sides over finite rings and fields of cardinality $q > 2$ is observed at the present time.

In [5, 6], analytical estimates of the reliability of reconstruction of the true solution of a system of linear equations with corrupted right sides over a ring $Z/(2N)$ are obtained by the method of maximum likelihood, and modifications of this method are proposed that have a smaller time complexity than the classical variant of its application. In [7], a method is proposed for the construction of new algorithms for the solution of the mentioned systems of equations from an arbitrary finite collection of such original algorithms. Analytical expressions for the reliability and time complexity of the algorithms obtained by this method are represented in terms of corresponding characteristics of the original algorithms, and a procedure is described for the construction of optimal (according to the criterion of the minimum laboriousness of these algorithms for a given lower reliability bound) algorithms in a definite class of algorithms for solving equations with corrupted right sides over the ring $Z/(2N)$.

Investigations of Boolean matrices and systems of linear equations over finite fields and rings. In [8], I. N. Kovalenko proves invariance theorems for a random Boolean determinant and investigates problems on the rank of a random matrix and on the distribution of the rank of lines of a random matrix with allowance for the rate of convergence to limit values. A. A. Levitskaya investigates systems of linear equations over finite rings in [8]. A number of results in invariance theory are obtained in works of V. I. Masol. A review of works on the investigation of systems of random equations over finite algebraic structures up to 2004 is presented in [12].

In [9], using the method of lattice moments (see below), A. N. Alekseychuk shows that the limit (as $n \to \infty$, $s = \text{const}$) distribution of the number of solutions of a system of linear equations $Ax = 0$ over the residue ring modulo p^d (p is prime and d is natural), where A is a random equiprobable matrix of size $(n + s) \times n$, is uniquely determined by the sequence of its moments if and only if we have $d \leq 2$.

In [10], the results of investigations of the distribution of the rank of an $(n + s) \times n$-matrix A with rows independent in aggregate over a field consisting of q elements. In terms of Fourier coefficients of distributions of rows for this matrix, upper and (in the case when Fourier coefficients are nonnegative numbers) lower estimates of probabilities of values of its rank are obtained. The upper bound is also obtained for the variation distance between distributions of ranks of the matrix A and ranks of a random equiprobable matrix. The condition is formulated according to which this variation distance tends to zero as $n \to \infty$, $s = \text{const}$, and it is shown that this condition cannot be weakened in a natural sense. A distinction of [10] from previous works on this topic lies in a greater generality of the problem statement and in a new method of investigation connected with Fourier coefficients, and the estimates obtained in it are more exact in some cases in comparison with the well-known estimates of G. V. Balakin [11].

In the review [12], the results of an investigation of matrices and their ranks, determinants, and methods of solution of systems of linear equations over finite algebraic structures are also presented.

Investigation of logical nonlinear equations and also equations over groups. In [8], systems of random logical equations are introduced and the probability of consistency and also the probability of uniqueness of solution of nonlinear systems of random equations is investigated. For systems of linear equations in a finite Abelian group, estimates are found for the average number of solutions and the distribution of the number of solutions for a primary group and cases of cyclic groups are investigated. The results have asymptotic character. The proved theorems may be thought of as the discovery of a new line of investigations in discrete mathematics. Nonlinear equations over finite fields were considered in works of V. I. Masol and his disciples. Invariance theorems for systems of random nonlinear equations over an arbitrary finite ring with left unity are proved in [74].

Probability distributions over a lattice. Problem of moments. In [13, 14], A. N. Alekseychuk presents the results of investigating a general scheme of independent stochastic elements with values in a finite lattice. It is shown that, in terms of this scheme, a general formulation of some probabilistic-combinatory problems is possible (on the distribution of probabilities of the number of uncovered points in a generalized scheme of placement of particles by sets, the number of connectivity components in a random hypergraph, the number of solutions of a system of random linear equations over a finite ring with unity, etc.). A method is also proposed for the proof of theorems on the convergence of sequences of random quantities ξ_n assuming values in a set $(0, 1, \dots, n)$ to discrete probability distributions. The method is based on the investigation of asymptotic behavior of definite numerical characteristics (lattice moments) of distributions ξ_n. Examples of usage of this method in investigating the asymptotic behavior of probability distributions of the dimension of the space of solutions to a system of independent random homogeneous linear equations over a finite field and also of the number of connectivity components of nonequiprobable random hypergraph with independent hyperedges are considered. In [15], the results are presented that develop and extend some statements obtained in [13, 14]. In particular, the concept of a covering index is introduced for a finite homogeneous lattice of rank n and the theorem on the asymptotic normality of the number of blocks in a random equiprobable covering of this lattice is proved. With the help of the method of lattice moments, a kind is found in [14] for the limit (as $n \to \infty$) law of distribution of the index of covering the lattice of a subspace of an n-dimensional vector space over a finite field.

It may be noted that the method of lattice moments was developed during investigations directed toward searching for general sufficient uniqueness conditions for the problem of moments in the class of q-distributions, i.e., discrete probability distributions that are concentrated on the set of powers of a number $q > 1$ with nonnegative integer indices [16]. An example of an q-distribution is the limit (as $n \to \infty$) distribution of probabilities of the number of solutions to a system consisting of $n + s$ random homogeneous linear equations of n unknowns over a field with q elements (s is an integer constant). For a long time, the question whether the mentioned distribution is uniquely determined by the sequence of its moments remained open. An answer in the affirmative is given in [16] in which sufficient conditions for the uniqueness of the problem of moments are obtained for probability distributions concentrated on a set of vectors $(q_1^{n(1)}, \ldots, q_t^{n(t)})$, $q_i > 1$, $n(i) \in N_0$, $i = 1, 2$.

Investigation of methods for calculating the number of complete mappings of finite sets. The methods developed in [17–19] for the estimation of the number of the so-called complete mappings constitute a significant advance in solving the problem that faced specialists in the field of applied mathematics and cryptographic methods of information protection over almost three decades. A new efficient approach [20] is proposed to the estimation of the number of complete mappings by the method of fast simulation that made it possible to estimate the number of complete mappings for $N = 205$ with the relative error 5%. Empirical upper and lower estimates of their number are also given. This problem is motivated by information protection problems. In decoding (cracking) enciphering systems such as, for example, “Enigma,” complete mappings (permutations without “parallelism,” i.e., without “special” coincidences) play an important part.

Problem of the distribution of identification codes. We assume that several users (independently of one another) choose an address or a code for themselves. The following question arises: what is the probability that some users will have the same address? An investigation of this question about collisions is pursued in [21]. Estimates of this probability are of great importance for correct construction of reliable access procedures in automated and computer systems. At present, with the rapid development of telecommunications, global computer networks, and systems of e-payments, the question of code distribution becomes most topical. Unimprovable asymptotic estimates for the minimum number of users for which the probability of a collision is no less than a prescribed probability are obtained in [76].

Probabilistic methods of generation of irreducible polynomials. In [22], probabilistic tests checking an integer for primality are generalized with a view to checking polynomials over Galois fields for irreducibility. The tests of Fermat, Solovey–Strassen, and Miller–Rabin are generalized and domains are specified in which the developed methods of generation of irreducible polynomials are more efficient than deterministic methods.

THEORY OF RANDOM DISTRIBUTIONS

Depending on applications, characteristics to be investigated, traditions, mathematical schools, and some other reasons, a large class of combinatorial problems can be formulated and investigated using various mathematical terminologies and can be interpreted with the help of various combinatorial configurations and schemes. The most important combinatorial configurations are particle placements between cells, samplings or urn schemes, and mappings of finite sets and graphs.

Depending on whether we consider particles or cells as ordered or unordered or as distinguishable or indistinguishable from one another, based on constraints on a placement, we will obtain various placement schemes. Accordingly, the number of all possible placements will also vary. For example, if cells are different and are not ordered and particles are not different, the number of possible placements equals C_{N+n-1}^{n}, where N is the number of cells and n is the number of particles. This corresponds to a commutative asymmetrical N-basis in terms of mappings and also to the Bose-Einstein statistics in statistical physics. On the set of all possible placements of a given combinatorial scheme, various probability distributions can be specified and, as a result, a wide variety of random schemes of placement of particles can be obtained each of which, as a rule, can be numerously used in applied problems of computer engineering, in mathematical methods of information protection, in physics, biology, etc. The conclusions and results obtained for placement schemes are used for the investigation of some discrete models and probabilistic combinatorial algorithms used in the synthesis and analysis of cryptographic systems of information protection, in various cryptanalysis methods, etc.

Scheme of random placement of particle sets between cells. n particle sets consisting of m particles are placed between cells and, in each set, particles are placed between cells containing no more than one particle, all C_N^m possible placements are equiprobable, and placements of particles between different sets are independent. (If $m = 1$, then we have the classical placement scheme.) We denote by $\mu_r(N, m, n)$ a random quantity equal to the number of cells that contain exactly r particles after placement of all n sets, by $\xi_r(N, m, n)$ a random quantity equal to the number of cells each of which contains no more than r particles after placement of n sets, and by $\nu_r(N, m, k)$ a random quantity equal to the least number of placed sets for which some k cells contain no less than r particles.

Using schemes of placement of particles by sets, mixed factorial and second moments and also distributions of random quantities and random vectors connected with the quantities $\mu_r(N, m, n)$, $\xi_r(N, m, n)$, and $\nu_r(N, m, k)$ are investigated in [8, 23]. A normal approximation is obtained for a multidimensional hypergeometric distribution with random parameters. Theorems on limit Gaussian and Poisson distributions and also on exponential and twice exponential limit distributions for waiting time are proved. In [25], a collection of limit theorems for the waiting time before filling given subsets of cells in the problem on the placement of particles by ses is presented. In [27], the asymptotic results obtained for maximal and minimal frequencies in the classical placement scheme are generalized to the case of a scheme of placement of a random number of particles.

In [8], with the help of combinatorial analysis of series, exact formulas are obtained for moments of arbitrary order of the maximum of two and three independent Gaussian random quantities and also for central moments of these quantities.

Placement of particle sets on a circle. In [8, 23], a scheme of placement of particle sets on a circle is described and investigated. In contrast to the classical placement scheme, random quantities connected with characteristics of the intersection of sets are introduced here. With the help of the theory of series, generating functions, and combinatorial-probabilistic analysis, the limit behavior of moments and distribution of random quantities are investigated and the convergence of distributions to Gaussian distributions and also to compositions of Poisson distributions is proved. The presented placement scheme is used in analyzing detectors of pseudorandom sequences that, as is well known, have a definite period.

Weak convergence of vector random processes in placement schemes to Gaussian diffusion processes. In [8, 23], a method is developed for the proof of the weak convergence of vector random processes constructed according to placement schemes in the space of functions without nonremovable discontinuities. The method is based on the use of general limit theorems of the theory of random processes. In [8, 23, 28], using the developed method, the convergence of vector random processes with two types of time orientation that are constructed according to various placement schemes to Gaussian diffusion processes is proved. Corollaries are obtained from functional limit theorems concerning the asymptotic behavior of joint distribution of random quantities, which provides one more method of proving multidimensional Gaussian limit theorems in placement schemes.

Nonequiprobable schemes. Separable statistics. A regular scheme of independent placement of n particles between N numbered cells is described as follows: independently of one another, each particle is placed with probability q_k in the cell with a number k, $k = \overline{1, N}$, $\sum_{k=1}^{N} q_k = 1$; as $N \to \infty$ and when $c_1, c_2 = \text{const}$ and $0 < c_1 < c_2$, the inequalities $0 < c_1 \le \min_k Nq_k \le \max_k Nq_k \le c_2 < \infty$ are fulfilled. Using the method proposed in [8, 23], the weak convergence is proved in [28] for multidimensional random processes constructed in a regular scheme from separable statistics in the space of functions without nonremovable discontinuities to a vector-valued Gaussian diffusion process. In [24], weak convergence is considered in the scheme of placement of particles by sets with random levels (specified over cells by another placement scheme).

Variational series of probabilities. If, in realizing the polynomial scheme, only the cases of appearance of m pairwise different outcomes (vectors $(i_1, \ldots, i_m)$) are considered, then, for an arbitrary fixed γ, $0 < \gamma < 1$, a quantity $N(\gamma)$ can be defined as the least possible number of vectors such that the sum of their probabilities will be no less than γ. The function $N(\gamma)$ depends on γ, N, and m and probabilities p_i of the polynomial scheme, $i = 1, \ldots, N$. This model is used, for example, in generating random samples without repetition, random placements of particle sets between cells, in constructing random functions, some commutation schemes, generators of random numbers, etc. In [26], some nonequiprobable variants of this scheme are investigated.

COMBINATORIAL-PROBABILISTIC ALGORITHMS FOR DETERMINATION OF PROPERTIES OF (0,1)-SEQUENCES AND BOOLEAN FUNCTIONS

Investigation of random and pseudorandom sequences. The determination of statistical and cryptographic characteristics of random and pseudorandom sequences and also generators of such sequences is one of the most important problems in constructing and applying cryptographic means and methods of information protection. In [29], statistical algorithms are constructed for the determination of switching moments of some alternating random process. In [30], a sequence of Bernoullian random quantities u_t, $t = \overline{1, N}$, such that $\mathbf{P}(u_t = 0) = \frac{1}{2}(1 + \Delta_t)$, $|\Delta_t| < 1$, $t = \overline{1, N}$, is considered and a sequence of Boolean random quantities $v_t = u_t \oplus u_{t - l_1(t)} \oplus \ldots \oplus u_{t - l_{m_t}(t)} \oplus \varphi(t)$, $t = \overline{1, N}$, constructed with the help of u_t is investigated, where $\varphi(t)$ is a nonrandom function of t with values in $\{0, 1\}$, $1 \le l_1(t) < l_2(t) < \ldots \ldots < l_{m_t}(t) \le t - 1$.

In [31], a new statistical criterion is proposed for checking random and pseudorandom sequences for quality. One of the most efficient compression algorithms is the method of contextual modeling. This method of information compression can be used for checking a sequence for randomness. The essence of the algorithm is as follows: in scanning the sequence from left to right, it is possible to make definite forecasts concerning succeeding symbols. The number of correct forecasts determines probabilistic characteristics of the algorithm. A theoretical and experimental analysis of a variant of this algorithm is presented in [67].

Multidimensional statistical criteria for checking random and pseudorandom sequences for quality that are constructed on the basis of limit theorems on weak convergence of vector random processes in placement schemes are investigated in [68].

On the independence of statistical tests. In [32], an adequate mathematical model is developed and definitions are formulated and proved for pairwise independence and independence in the aggregate of statistical tests destined for checking generators of random, pseudo-random, and individual sequences and also the block of generation of the gamma of a stream cipher for quality; the methodology of checking statistical tests for independence and the methodology of formation of a collection of such tests are presented.

In [33], questions of generation of nonequiprobably distributed key parameters are considered.

Statistical definition of properties of Boolean functions. In [34], methods of statistical determination of special cryptographic properties of multidimensional Boolean functions are proposed. Such functions can describe the functioning of units of discrete devices, finite-state machines, cryptographic transformations, etc. For example, a block encoder realizes such multidimensional Boolean functions in the mode of an electronic code book.

In a software or a hardware realization of complicated Boolean functions of many variables, the problem of checking such a realization for correctness arises, i.e., that of the identity of a Boolean transformation of some standard Boolean function. The realization of this check for a large number of variables by an exhaustive search over all possible inputs is problematic even for modern computer engineering. In [34], probabilistic tests are proposed and proved that, using the Monte Carlo method, establish the identity or dissimilarity of vector-valued Boolean functions of many variables with parameters and a given confidence probability α and a maximal risk β.

Cryptanalysis of stream encoders. Several years ago, a new cryptanalysis method arose whose essence lies in simplifying (by a special method) and subsequently solving a system of equations that describes the functioning of an encoder (key bits are unknown variables of the system). This method was called the method of algebraic attacks.

First essential results in the cryptanalysis of real encoders with the help of algebraic attacks were obtained in 2002. N. Courtois proposed a "higher order correlation attack" on the stream encoder "Toyocrypt" (presented for a competition between encoders at "Cryptrec"). A new improved algebraic attack produced a new system of equations for "Toyocrypt" with the complexity of solution equal to 2^{49} operations. This approach was improved later on and a "fast algebraic attack" made it possible to reconstruct the key of this encoder using 2^{20} operations (if there are about 300 KB of continuous gamma and at the stage of preliminary calculation with 2^{23} operations). Later on, an efficient algebraic attack on block encoders was investigated.

In [35, 36], a description of an algebraic attack on stream encoders with the help of conditional correlation is presented. This made it possible to generalize the concept of the *k*th order nonlinearity of a Boolean function. This concept is used, in particular, in higher order correlation attacks. An example of a filtering function is presented. This function is very vulnerable to a higher order correlation attack that uses the introduced "partial nonlinearity" but is weakly vulnerable to an attack of the same type with the use of the conventional *k*th order nonlinearity. An efficient algorithm is also developed (and the corresponding program is written) for checking a Boolean function $f(\bar{x})$ for the presence of *k*th order approximations that strongly correlate with f in terms of conditional correlation. In the case of existence of good approximations, the algorithm finds the best of them. For cryptanalysis, methods for the solution of systems of linear equations (with corrupted right sides) over finite fields were also used.

In [36], algebraic attacks on stream encoders were investigated. The concepts of conditional correlation and partial nonlinearity of Boolean functions are introduced, and also concepts of algebraic immunity are extended. This makes it possible to unify the description of deterministic and probabilistic scenarios of algebraic attacks (we note that probabilistic scenarios were investigated for the first time). A simple criterion of vulnerability of a function to a probabilistic attack scenario in terms of conditional correlation is given. A definite set of functions vulnerable to a probabilistic attack scenario is constructively constructed and it is illustrated by their examples that, for some complicating functions, such an attack scenario is most efficient.

In [37], the key of the stream encoder "SFINKS" with a weakened filtering function is experimentally found with the help of a probabilistic algebraic attack. The class of such vulnerable functions is rather wide and contains many functions resistant against well-known nonalgebraic methods of cryptanalysis. In [38], new theoretical concepts are introduced for Boolean functions, namely, the correlation when the value of a function is known and an extension of a Boolean function. It is proved that an algebraic attack on memoryless stream encoders is reduced to the approximation of complication functions of an encoder by lower-order polynomials in terms of the introduced correlation. This correlation can also be used for the description of algebraic attacks on other types of encoders. In [39], estimates of cardinalities of classes of Boolean functions of *n* variables whose algebraic immunity does not exceeds *k* are obtained. The results are useful in investigating algebraic attacks on stream encoders. The essence of algebraic attacks on stream ciphers lies in lowering the degree of a system of equations connecting bits of an unknown key with known output bits of the cipher by a definite method. Probabilistic scenarios of an attack presume even a greater decrease in the degree but, in this case, the obtained equations are true not for all arguments. In [40], scenarios are investigated and corresponding concepts are introduced in terms of which the resistance of a complicating Boolean function of a stream cipher against this form of attacks is easily described.

The theory of statistical methods of cryptanalysis of stream ciphers is developed in [41–44] in which a probabilistic model of functioning in the mode of reinitialization of the initial state of combining gamma generators with nonuniform data movement in shift registers is proposed and investigated in detail. It is shown that the resistance of such generators against some statistical attacks is determined by a collection of conditional probabilities for which explicit analytical expressions [42, 44] are obtained. These expressions allow one to establish a close relationship between the following two cryptoanalytical problems that are different at first sight: the reconstruction of values of the combining function of a gamma generator with nonuniform movement and reconstruction of messages corrupted during their transmission along a discrete tapped communication channel [45–47]. The presence of such a relationship allows one to extend the well-known results obtained earlier for random coding systems to the class of gamma generators being considered and, in particular, to obtain a general sufficient optimality condition (according to the minimum reliability criterion for reconstruction of values) for the combining function of a gamma generator with nonuniform data movement in shift registers [41, 44].

Some modern methods of cryptanalysis of stream ciphers are also investigated in [48].

Investigations of block encoders. New approaches to the cryptanalysis of block ciphers and their resistance against linear and differential analysis are investigated by A. N. Alekseychuk and L. V. Koval'chuk. In particular, the concept of a "non-Markov" cipher is proposed that allows one to more adequately describe some types of ciphers. Methods of substantiation of the practical resistance of non-Markov block ciphers against difference (differential) and linear cryptanalysis are developed in [49–54]. In [49], analytical upper bounds are obtained for maxima of probabilities of differential and linear characteristics of the Feistel cipher containing a key adder modulo 2^m (an example of this cipher is the standard GOST 28147–89). The expressions for the upper bounds contain new numerical parameters of replacement units of this cipher that are different from the classical parameters traditionally used for the estimation of practical resistance of Markov block ciphers against differential and linear cryptanalysis methods. In [50, 51], analytical upper estimates are obtained for the probabilities of differential approximations of transformations of the form $(x,k) \mapsto \varphi(x+k)$, x, $k \in \{0, 1\}^m$, where φ is a substitution on the set $\{0, 1\}^m$, and the sign + denotes the modulo 2^m operation of addition of integers corresponding to binary vectors. The mentioned estimates are constructed for various variants of definition of group operations over the domain and codomain of the transformations being investigated. Further refinements of these estimates for a wide class of the so-called generalized Markov ciphers are obtained by L. V. Koval'chuk in [53]. To date, the most exact upper bounds of the parameters characterizing the practical resistance of GOST-like block ciphers against methods of differential and linear cryptanalysis are presented in [54]. These bounds allows one to majorize the upper bounds for maximal values of probabilities of differential and linear characteristics of the cipher GOST 28147–89 (under definite but not too rigid constraints on the choice of its replacement units) by the numbers 2^{-56} and 2^{-42}, respectively.

The methods developed in [49–54] are successfully applied in [55] to the investigation of the resistance of one more important class of block ciphers constructed with the use of a modulo 2^m key adder, namely, to the cipher "Kalina," which is a candidate for a national standard of enciphering in Ukraine, and to its analogues. In particular, the estimates of probabilities of differential and linear characteristics of the cipher "Kalina" that are obtained in [55] allow one to substantiate its practical resistance against methods of differential and linear cryptanalysis without any simplifying assumptions.

In [56], A. N. Alekseychuk and A. S. Shevtsov obtained new upper bounds for the reliability of first-order statistical attacks on arbitrary block ciphers. These bounds allow one to introduce justified indices of resistance of block ciphers against a wide class of (linear, generalized linear, bilinear, etc.) attacks without resort to traditional heuristic assumptions. At the same time, in the case of a linear distinguishing attack, the new estimate of resistance [56] is one or two orders of magnitude more exact than the estimate well known earlier [57].

A differential analysis of the standard GOST 28147-89 is also performed in [58].

In [59, 60], S. V. Jakovlev presents the results of investigation of an important part of the standard GOST 28147–89, namely, the so-called S-blocks that form a long-term private key. Criteria are formulated for the selection of substitutions in S-blocks that guarantee, on the one hand, a high reliability and, on the other hand, a large cardinality of the key space, algorithms of generation of long-term keys are constructed, and the resistance of S-blocks against attacks of linearization and correlation, linear, and differential analysis and also against differential power and timing attacks. Note that the approved algorithms for generating long-term keys of the standard GOST 28147–89 have not been published neither in Russia nor in Ukraine.

In [61], a new construction of block ciphers, namely, the Feistel cascade scheme is proposed, and estimates of differential and linear characteristics of this scheme are obtained. S. V. Yakovlev performed a comparative analysis of the design of the cipher “Kalina” and ciphers *AES* and *W*. The compliance of the cipher “Kalina” with the requirements on a plausible candidate for the national enciphering standard is investigated.

Cryptanalysis of enciphering algorithms based on deterministic chaos. Recently, attempts are made to use new results of various scientific directions in cryptography. One of such directions is the theory of deterministic chaos.

In [62–64], a cryptosystem with the public key based on a piecewise linear mapping used in chaotic dynamics and also a modification of a cryptosystem in which lower order bits of the floating-point binary representation of a number (standard IEEE 754) are eliminated are analyzed. Based on the results of investigation of the functionality of such a system and properties of the mapping $T_k(x) = \frac{1}{\pi} \arccos(\cos(k\pi x))$ being used, the possibility of realization of a successful and efficient keyless attack is shown. A message reconstruction algorithm without knowledge of private keys is presented, and also main drawbacks that lead to the breaking of the system are considered.

Locally-commutative symmetric ciphers in asymmetric cryptography and their resistance in a postquantum model of computations. In [65, 66], it is proposed to use commutative and locally-commutative symmetric ciphers resistant to plain-text attacks to construct one-sided functions and asymmetric cryptoschemes. With allowance for the properties of such ciphers, analogues of the majority of well-known asymmetric protocols (of Diffie-Hellman, Al–Gamal, Schnorr, etc.) were constructed. The resistance of such functions in the classical model of computations is analyzed and their postquantum vulnerability is proved by reducing the problem of inversion of such a function to a special case of the hidden subgroup problem when there is a solution in the framework of the quantum model of computations.

Investigation and development of cryptographic standards. Over a period of years, investigations on the harmonization of the European cryptographic standards were carried out in the Cybernetics Institute of NASU with a view to using them in Ukraine under the conditions of the Ukrainian normative base and technical and organizational capabilities. According to the plans of the state standardization of Ukraine, eight ISO/IEC standards were developed and harmonized in 2004-2009 under contracts between the Ukrainian Research Institute for Standardization, Certification & Informatics, the State Committee of Ukraine for Technical Regulation and Consumer Policy, and the Technical Committee on Standardization “Information Technologies” (TK-20) with the participation of A. V. Anisimov, A. M. Fal’, V. V. Tkachenko, et al. with a view to accepting them in Ukraine [69–71]. Specialists of the Cybernetics Institute of NASU continue to investigate and harmonize other ISO/IEC standards, they also investigated and developed digital signature algorithms [72]. A. I. Kochubinskii and A. S. Shatalov developed a national digital signature standard based on elliptic curves [73].

Scientific seminar “Problems of modern cryptology.” The size of this article makes it impossible to present all the results on theoretical cryptography that are obtained even only by the specialists of the Kiev cryptographic school within the last twenty years. We would like to note works of A. V. Anisimov, V. K. Zadiraka, V. A. Mukhachev, A. I. Kochubinskii, A. M. Kudin, and many others. The last articles of A. N. Alekseychuk, P. A. Endovitskii, and A. A. Levitskaya that are devoted to theoretical cryptography [75–77] are published in this issue of the journal. An idea of the variety of lines of investigations is given by the titles (listed below) of the reports presented at the Kiev scientific seminar “Problems of modern cryptology” within the past nine years (unfortunately, we failed to restore titles of some reports).

30.11.2001. **A. N. Alekseychuk and O. I. Romanov** (Kiev), “Regular congruences and the structure of algebraic models of symmetric cryptosystems.”

13.12.2001. **R. V. Oleinikov** (Kharkov), “Analysis of resistance and conditions of application of GOST 28147–89;” **S. A. Golovashich** (Kharkov), “Methods of construction of highly resistant symmetric ciphers and schemes for applying them.”

27.12.2001. **A. N. Alekseychuk** (Kiev), "'Lattice' moments of integer-valued nonnegative random quantities and their use in solving problems of probabilistic combinatorics."

17.01.2002. **A. B. Telizhenko** (Kiev), "Random search algorithms and their application to cryptography."

31.01.2002. **M. N. Savchuk** (Kiev), "On algorithms for solution of systems of linear equations with corruptions."

14.02.2002. **K. A. Romanovich** (Kiev), "Methods for solution of random systems of pseudo-Boolean equations."

28.02.2002. **A. M. Fal** (Kiev), "A comparative review of international cryptography standards."

14.03.2002. **A. I. Kochubinskii** (Kiev), "Comparison of standards of Ukraine and the Russian Federation on the basis of elliptic curves."

28.03.2002. **R. V. Oleinikov** (Kharkov), "Differential cryptanalysis of the enciphering standard GOST 28147–89."

11.04.2002. **A. A. Levitskaya** (Kiev), "Invariance theorems for random nonlinear systems of Boolean equations."

25.04.2002. **N. N. Budko, V. S. Vasilenko, and M. P. Korolenko** (Kiev), "Monitoring and restoration of information integrity in automated systems."

26.09.2002. **I. N. Kovalenko** (Kiev), "Recollections on the Kiev and Moscow mathematical and cybernetic schools and a view of the modern state and prospects in some lines of investigations."

10.10.2002. **L. V. Koval'chuk** (Kiev), "Pseudoirreducible polynomials: Probabilistic testing of the irreducibility of polynomials."

24.10.2002. **I. N. Kovalenko** (Kiev), "Some problems of probabilistic combinatorics."

07.11.2002. **A. M. Kudin** (Kiev), "Estimation of the resistance of cryptosystems using the Chebyshev radius of information."

21.11.2002. **S. V. Bulygin** (Kiev), "Estimation of a cryptographic function using the technique of algebro-geometrical codes."

05.12.2002. **V. B. Ufimtseva** (Kharkov), "Application of Fibonacci Q-matrices in exchange schemes of the Feistel network."

19.12.2002. **V. K. Zadiraka** (Kiev), "Spectral methods in steganography."

16.01.2003. **V. K. Zadiraka and N. V. Borodavka** (Kiev), "A software implementation of a spectral algorithm for construction of a digital container."

30.01.2003. **E. A. Lebedev** (Kiev), "Algorithms for calculation of basic distributions of applied statistics."

13.02.2003. **A. V. Bessalov** (Kiev), "Application of elliptic curves to cryptography: Elliptic curve digital signature standards."

13.03.2003. **L. A. Zavadskaya and A. S. Mellit** (Kiev), "On the cryptanalysis of stream enciphering schemes."

27.03.2003. **A. F. Turbin and A. P. Velikii** (Kiev), "On the Lobanov transform."

10.04.2003. **N. M. Glazunov** (Kiev), "Algebraic curves and cryptography."

24.04.2003. **A. S. Mellit** (Kiev), "On a realization of the Sat algorithm for calculation of the order of points of an elliptic curve;" **S. N. Torba** (Kiev), "Efficient exponentiation of points of an elliptic curve with the operation of division of a point by two."

19.10.2003. **A. N. Alekseychuk** (Kiev), "Analysis of the resistance of randomized block encoders to the differential cryptanalysis."

23.10.2003. **L. V. Koval'chuk** (Kiev), "Probabilistic testing of the irreducibility of polynomials."

06.11.2003. **V. I. Masol** (Kiev), "Asymptotics of distributions for some characteristics of random matrices over a finite field."

20.11.2003. **A. N. Alekseychuk** (Kiev), "Random coverings of a homogeneous finite lattice."

04.12.2003. **A. I. Kokhanovskii** (Kiev), "Problem questions of information protection in electronic document management systems."

15.01.2004. **N. V. Borodavka** (Kiev), "Steganogrammas based on the convolution theorem."

29.01.2004. **B. A. Bredelev** (Kiev), “Steganographic systems within the framework of models of passive and active adversaries.”

12.02.2004. **A. Zubenko** (Kiev), “Information protection schemes in dynamic environments.”

26.02.2004. **S. N. Konyushok** (Kiev), “Construction of key distribution schemes with the theoretical resistance based on combinatorial configurations.”

11.03.2004. **A. M. Kudin and A. A. Dovyd’kov** (Kiev), “Construction of integrated protection systems for distributed automated systems whose architectures dynamically vary.”

25.03.2004. **M. N. Savchuk** (Kiev), “Cryptographic properties of Boolean functions.”

22.04.2004. **A. A. Dovyd’kov** (Kiev), “Approaches to the simulation of security policies of computer systems.”

30.09.2004. **I. N. Kovalenko** (Kiev), “Operational experience in the field of applied probability theory and mathematical statistics.”

14.10.2004. **A. N. Alekseychuk** (Kiev), “A statistical cryptanalysis method for gamma generators constructed from linear registers with nonuniform movement.”

28.10.2004. **L. V. Koval’chuk** (Kiev), “Application of the Pollard method for finding collisions of hash functions.”

11.11.2004. **A. V. Bessalov** (Kiev), “A method of division of points by 2 as applied to elliptic curve cryptography.”

25.11.2004. **L. V. Koval’chuk and V. T. Bezdetnyi** (Kiev), “A methodology of checking tests for ”independence" with a view to testing generators of pseudorandom sequences."

23.12.2004. **A. L. Voloshin** (Kiev), “A linear scheme of distribution of a secret over a residue ring modulo a primary module.”

20.01.2005. **A. N. Alekseychuk** (Kiev), “Universal algebras and secrets distribution schemes.”

03.02.2005. **V. A. Ustimenko** (Kiev), “Walks on graphs and cryptography.”

17.02.2005. **V. K. Zadiraka and A. M. Kudin** (Kiev), “Hardware-software system of multiprecision arithmetic.”

03.03.2005. **A. N. Alekseychuk and S. M. Ignatenko** (Kiev), “Systems of linear equations with corrupted right sides over the residue ring modulo 2^n.”

17.03.2005. **I. Ya. Kinakh** (Ternopol), “A model of parallel realization of the general number field sieve;” **B. Z. Karpinskii** (Ternopol), “High-performance stream ciphers with improved resistance against attacks.”

31.03.2005. **S. A. Pometun**, (Kiev), “Algebraic attacks on stream ciphers;” **Kudin A.M.** (Kiev), “An approach to the hardware implementation of algorithms of multiword arithmetic. I.”

14.04.2005. **A. M. Kudin** (Kiev), “An approach to the hardware implementation of algorithms of multiword arithmetic. 2.”

29.09.2005. **I. N. Kovalenko** (Kiev), “On the functioning of the International Conference ”Modern problems and new lines of investigations in probability theory" and its section “Probabilistic and statistical methods in cryptography” (held in Chernovtsy); **V. K. Zadiraka** (Kiev), “Communication on the 32nd conference on the optimization of computations devoted to V. S. Mikhalevich (held in Katsiveli);” **A. V. Anisimov** (Kiev), “Investigations in the field of mathematical methods of information protection at the Faculty of Cybernetics of the National Taras Shevchenko University of Kiev.”

13.10.2005. **A. N. Alekseychuk and L. V. Koval’chuk** (Kiev), “Upper bounds for maximal values of probabilities of differential and linear characteristics of a Feistel-type encoder with a modulo 2^n adder.”

27.10.2005. **E. V. Gomonai and A. V. Fesenko** (Kiev), “Efficient algorithms for quantum computation and their application to cryptography.”

10.11.2005. **I. A. Zavadskii** (Kiev), “Grover’s search algorithm.”

24.11.2005. **A. A. Polyakov** (Kharkov), “Generation of system parameters for elliptic curves.”

08.12.2005. **A. V. Fesenko** (Kiev), “Shor’s quantum algorithm for factoring integers.”

22.12.2005. **D. S. Balagura** (Kiev), “Analysis, comparison, and improvement of cryptographic protocols for installation of keys used in information-computing systems (ICSs).”

02.03.2006. **S. V. Yakovlev** (Kiev), “Criteria of selection and an algorithm for generating long-term keys according to GOST 28147-89.”

16.03.2006. **B. A. Bredelev** (Kiev), “A steganographic algorithm resistant to a number of statistical attacks.”

30.03.2006. **A. Ya. Beletskii** (Kiev), “A family of symmetric block cryptographic algorithms for information protection.”

13.04.2006. **S. A. Pometun** (Kiev), “Construction of algebraic attacks using conditional correlation.”

27.04.2006. **A. Ya. Beletskii** (Kiev), “Generalized Grey codes and their use in information protection schemes.”

11.05.2006. **A. V. Antonov** (Kharkov), “Cryptographic functions with a secret based on an information complexity measure of inversion of chaotic mappings.”

02.11.2006. **L. V. Koval’chuk** (Kiev), “Generalized Markov ciphers: An estimate of their resistance to differential cryptanalysis.”

16.11.2006. **A. N. Alekseychuk and R. V. Proskurovskii** (Kiev), “Statistical attack on combined gamma generators with nonuniform movement in the mode of reinitialization of the initial state.”

30.11.2006. **A. Ya. Beletskii** (Kiev), “RSB technology of construction of symmetric block cryptographic algorithms.”

14.12.2006. **V. E. Fedyukovich** (Kiev), “Partial coincidence of sets without disclosure.”

15.02.2007. **V. E. Fedyukovich** (Kiev), “Methodology for demonstration of partial coincidence of sets.”

01.03.2007. **A. M. Fal’** (Kiev), “A review of international standards on information technology security.”

15.03.2007. **I. D. Gorbenko, V. I. Dolgov, and R. V. Oleinikov** (Kharkov), “Principles of construction and specification of the block encoder ‘Kalina’ submitted to a competition.”

29.03.2007. **N. V. Koshkina** (Kiev), “Methods of synchronization of digital watermarks.”

12.04.2007. **N. Yu. Kuznetsov** (Kiev), “Using fast simulation for determination of the number of ”good" permutations."

26.04.2007. **A. V. Fesenko** (Kiev), “Cryptanalysis of enciphering systems constructed on the basis of dynamic chaos.”

11.10.2007. **S. A. Pometun** (Kiev), “Generalized correlation and high-order nonlinearity in algebraic attacks on stream encoders.”

25.10.2007. **V. K. Zadiraka, A. M. Kudin, and V. A. Lyudvichenko** (Kiev), “Computer technologies of cryptographic protection of information stored on special carriers.”

08.11.2007. **L. V. Koval’chuk** (Kiev), “Methods of analysis and synthesis of existing and promising byte-oriented stream cryptosystems for protection of state information resources.”

22.11.2007. **S. V. Popereshnyak** (Kiev), “Distribution of ranks of weakly and strongly filled matrices in the field *GF*(2);” **N. V. Slobodyan** (Kiev), “Approximation of the distribution of the number of false solutions of a system of nonlinear random equations in the field *GF*(2) by the Poisson distribution.”

06.12.2007. **A. A. Borisenko** (Sumy), “Analysis of cryptographic resistance of discrete information sources.”

20.12.2007. **A. M. Kovalyov, V. A. Kozlovskii, A. Ya. Savchenko, and V. F. Shcherbak** (Donetsk, Kiev), “New methods and algorithms of information transformation based on automaton-like and chaotic dynamic systems for digital processing, coding, storage, and efficient protection of information.”

14.02.2008. **V. A. Ustimenko** (Kiev, Donetsk), “Extreme graph theory and its cryptographic applications.”

28.02.2008. **A. N. Alekseychuk, L. V. Koval’chuk, and A. S. Shevtsov** (Kiev), “Generalized Markov ciphers ‘Kalina’ and ‘Mukhomor:’ Estimation of practical resistance to differential and linear cryptanalysis.”

13.03.2008. **S. A. Slobodyan** (Ivano-Frankovsk), “Theorems on normal limit distribution of the number of false solutions to a system of nonlinear random equations in the field *GF*(2).”

27.03.2008. **L. A. Zavadskaya** (Kiev), “Cryptanalysis of the stream cipher **RC**-4.”

10.04.2008. **A. V. Fesenko**, (Kiev), “Compromise attacks on stream cryptosystems;” **S. V. Yakovlev** (Kiev), “Side-channel attacks on stream encoders.”

24.04.2008. **V. G. Sharapov and V. E. Fedyukovich** (Kiev), “An interactive protocol for demonstration of multiple occurrences of a string.”

25.09.2008. **S. A. Pometun** (Kiev), “Algorithms of probabilistic algebraic attacks on stream ciphers.”

09.10.2008. **M. N. Savchuk and A. V. Fesenko** (Kiev), “Investigation of one-sided functions constructed from symmetric ciphers.”

23.10.2008. **K. Chernyakhovich and Yu. Yaremchuk** (Vinnitsa), “Elliptic curve digital signature methods with a fast procedure for verifying digital signatures.”

06.10.2008. **A. N. Alekseychuk** (Kiev), Theoretical bases for synthesis and substantiation of the resistance of randomized symmetric enciphering systems and key transmission and distribution protocols."

20.11.2008. **S. V. Yakovlev** (Kiev), “Construction of collisions for the hash function of the standard GOST P 34.311-95.”

04.12.2008. **V. E. Fedyukovich** (Kiev), “Proof and argument protocols: Elementary introduction and examples of problems being solved.”

18.12.2008. **M. K. Morokhovets** (Kiev), “Diagnostic experiments with finite automata.”

12.03.2009. **S. A. Pometun (**Kiev), “Algorithms for solution of systems of nonlinear equations with weakly corrupted right sides.”

26.03.2009. **V. E. Fedyukovich** (Kiev), “Algebraic operations over ciphertexts of the Paillier system and a protocol for proof of plaintext knowledge (based on P. Paillier (Eurocrypt 1999), Paillier-Pointcheval (Asiacrypt 1999), and Damgard-Jurik (PKC 2001)).”

09.04.2009. **P. A. Endovitskii** (Kiev), “A voting method in solving systems of equations.”

23.04.2009. **L. L. Nikitenko** (Kiev), “Investigation of a resistance criterion of steganosystems under passive attacks.”

15.10.2009. **A. M. Kudin** (Kiev), “Cryptographic transformations of non-Shannon information sources.”

29.10.2009. **L. A. Romashova** (Kiev), “On the probability of existence of solutions to a system of nonlinear random equations over the field $GF(3)$ in a given set.”

26.11.2009. **L. Ya. Glinchuk** (Lutsk), “Stern-Brocot cryptosystem and its application.”

10.12.2009. **S. V. Yakovlev** (Kiev), “Feistel cascade schemes and estimation of their resistance.”

24.12.2009. **P. A. Endovitskii** (Kiev), “Refinement of asymptotic approximation of the size of a group in the birthday paradox.”

REFERENCES

1. I. N. Kovalenko, “On an algorithm of subexponential complexity for decoding heavily corrupted linear codes,” Dop. AN URSR, Ser. A, No. 10, 16–17 (1988).
2. I. N. Kovalenko and M. N. Savchuk, “Some methods of decoding corrupted linear codes,” Data Registration, Storage, and Processing, **1**, No. 2, 62–68 (1999).
3. I. N. Kovalenko and M. N. Savchuk, “On a statistical algorithm to decode heavily corrupted linear codes,” in: Applied Probability and Stochastic Processes, Kluwer, Berkeley (1999), pp. 73–82.
4. K. Efremov and M. Savchuk, “Estimates of complexity and reliability of algorithms of decoding heavily corrupted linear codes,” in: Proc. IXth Intern. Sci.-Pract. Conf. “Information Security in Informational-Telecommunication Systems,” Kiev (2006), p. 24.
5. A. N. Alekseychuk, “Systems of linear equations with corrupted right sides over a residue ring modulo 2^N,” Zakhist Informatsii, No. 4, 12–19 (2001).

6. A. N. Alekseychuk and S. M. Ignatenko, “Estimates of efficiency of universal methods for reconstruction of corrupted linear recurrents over a residue ring modulo 2^N ,” Zbirn. Nauk. Prats’ of IPME of NANU, No. 20, 40–48 (2003).
7. A. N. Alekseychuk and S. M. Ignatenko, “Method of optimization of algorithms for solution of systems of linear equations with corrupted right sides over a residue ring modulo 2^N ,” Data Registration, Storage, and Processing, **7**, No. 1, 21–29 (2005).
8. I. N. Kovalenko, A. A. Levitskaya, and N. M. Savchuk, Selected Topics in Probabilistic Combinatorics [in Russian], Naukova Dumka, Kiev (1986).
9. A. N. Alekseychuk, “Uniqueness conditions of the moments problem in the class of *q*-distributions,” Diskret. Mat., **11**, No. 4, 48–57 (1999).
10. A. N. Alekseychuk, “Nonasymptotic bounds of the probability distribution of the rank of a random matrix over a finite field,” Diskret. Mat., **19**, No. 2, 85–93 (2007).
11. G. V. Balakin, “Systems of random equations over a finite field,” Trudy po Diskretnoi Matematike, **2**, 21–37 (1998).
12. A. A. Levitskaya, “Systems of random equations over finite algebraic structures,” Cybernetics and Systems Analysis, No. 1, 67–93 (2005).
13. A. N. Alekseychuk, “A probabilistic scheme of independent random elements distributed over a finite lattice. I. Exact probability distributions of functionals of union of random elements,” Cybernetics and Systems Analysis, No. 5, 629–638 (2004).
14. A. N. Alekseychuk, “A probabilistic scheme of independent random elements distributed over a finite lattice. II. The method of lattice moments,” Cybernetics and Systems Analysis, No. 6, 824–841 (2004).
15. A. N. Alekseychuk “Random covers of finite homogeneous lattices,” Theory of Stoch. Processes, **12(28)**, Nos. 1–2, 12–19 (2006).
16. A. N. Alekseychuk, “On uniqueness of the problem of moments in the class of *q*-distributions,” Diskr. Mat., **10**, No. 1, 95–110 (1998).
17. I. N. Kovalenko, “Upper bounds on the number of complete maps,” Cybernetics and Systems Analysis, No. 1, 65–68 (1996).
18. I. M. Kovalenko and C. Cooper, “The upper bound for the number of complete mappings,” Teor. Imovirn. Mat. Stat., **53**, 69–75 (1995).
19. C. Cooper, R. Gilchrist, I. N. Kovalenko, and D. Novacovic, “Estimation of the number of good permutations with applications to cryptography,” Cybernetics and Systems Analysis, No. 5, 688–693 (1999).
20. N. Yu. Kuznetsov, “Applying fast simulation to find the number of good permutations,” Cybernetics and Systems Analysis, No. 6, 830–837 (2007).
21. R. Gilchrist and I. N. Kovalenko, “On estimation of the probability of absence of collisions of some random mappings,” Cybernetics and Systems Analysis, No. 1, 102–107 (2000).
22. L. V. Kovalchuk, “Pseudoirreducible polynomials: Probabilistic irreducibility testing,” Cybernetics and Systems Analysis, No. 4, 610–616 (2004).
23. M. N. Savchuk, “Some limit theorems in the scheme of equiprobable placement of particles by sets,” Teor. Veroyatn. Mat. Stat., No. 28, 122–130 (1983).
24. M. Savchuk, “Some limiting theorems in ball batch allocation scheme with random levels defined by another allocation scheme,” in: Probabilistic Methods in Discrete Mathematics, Teor. Veroyatn. Prim., Moscow (1993), pp. 428–436.
25. M. N. Savchuk, “Limit behavior of a random waiting time before filling a given subset of cells in the scheme of equiprobable placement of particles by sets,” in: Models and Methods of Operations Research and Risk and Reliability Theories, Cybernetics Institute of NANU, Kiev (1992), pp. 3–10.
26. M. N. Savchuk, “Asymptotic analysis of a variational probability series for series with different outcomes in a multinomial scheme,” Dop. NAN Ukr., No. 3, 101–105 (1999).
27. M. N. Savchuk, “On limit distributions of maximal and minimal frequencies in a scheme of placement of a random number of particles among cells,” in: Mathematical Methods of Simulation and System Analysis under Conditions of Incomplete Information, Cybernetics Institute of AN UkrSSR, Kiev (1991), pp. 9–12.

28. M. N. Savchuk, “Convergence of multidimensional random processes connected with separable statistics in placement schemes to Gaussian diffusion processes,” in: Analysis of Stochastic Systems by Operations Research Methods and Reliability Theorems, Cybernetics Institute of AN UkrSSR, Kiev (1987), pp. 43–47.

29. M. N. Savchuk and V. F. Sinyavskii, “On an algorithm for determination of moments of changing parameters of a Bernoullian sequence,” Probl. Upravlen. Inf., No. 1, 84–89 (1999).

30. M. N. Savchuk, “Analysis of a method for improving characteristics of a random binary sequence,” Kibern. Vychisl. Tekhn., No. 118, 57–61 (1998).

31. V. Sharapov, “Algorithm for testing random and pseudorandom sequences using contextual simulation,” in: Proc. Xth Anniv. Intern. Sci. Pract. Conf. “Information Security in Informational-Telecommunication Systems,” ChP “EKMO” and NITs “Tezis” of NTUU “KPI,” Kiev (2007), pp. 30–31.

32. L. Koval’chuk and V. Bezditnyi, “Checking the independence of statistical tests destined for estimation of cryptographic properties of GPV,” Zakhyst Informatsii, No. 2 (29), 18–23 (2006).

33. L. Koval’chuk, S. Melnik, and V. Bezdetnyi, “Probabilistic characteristics of generation of nonuniformly distributed keys,” Radiotekhnika (Kharkiv), **141**, 181–188 (2005).

34. M. N. Savchuk, “Using the Monte Carlo method for identification of Boolean functions of a large number of variables,” Kibern. Vychisl. Tekhn., No. 117, 3–7 (1998).

35. S. A. Pometun, “Investigation of algebraic attacks on stream and block encoders,” in: Proc. Xth Anniv. Intern. Sci. Pract. Conf. “Information Security in Informational-Telecommunication Systems,” ChP “EKMO” and NITs “Tezis” of NTUU “KPI,” Kiev (2007), pp. 28–29.

36. S. A. Pometun, “Generalized higher-order correlation and nonlinearity of Boolean functions for the description of probability of algebraic attacks,” in: Proc. 3th Intern. Sci. Conf. on Problems of Security and Counteraction to Terrorism, in: MaBIT, Moscow (2007), pp. 153–163.

37. S. A. Pometun, “Probabilistic algebraic cryptanalysis of the encoder ‘SFINKS’ with a definite class of filtering functions,” Legal, Normative, and Metrological Support of the Information Protection System in Ukraine, No. 1 (16), 73–78 (2008).

38. S. A. Pometun, “Algebraic attacks on stream encoders as a generalization of correlation attacks,” Systemn. Doslidzh. to Inform. Tekhnologii, No. 2, 29–40 (2008).

39. S. A. Pometun, “On the number of Boolean functions with a given algebraic immunity,” Prikl. Radioelektronica, No. 3, 322–325 (2008).

40. S. A. Pometun, “Investigation of probabilistic scenarios of algebraic attacks on stream ciphers," Probl. Upravlen. Inf., No. 1, 143–156 (2009).

41. A. N. Alekseychuk and R. V. Proskurovskii, “Lower bound of the probability of distinguishing between inner states of a combining gamma generator with nonuniform movement,” in: Legal, Normative, and Metrological Support of the Information Protection System in Ukraine, No. 2 (13), Kyiv (2006), pp. 159–169.

42. A. N. Alekseychuk, R. V. Proskurovskii, and L. V. Skrypnik, “A statistical attack on a combining gamma generator with nonuniform movement in the mode of reinitialization of the initial state,” in: Proc. MGU Conf. “Mathematics and Security of Information Technologies,” MTsNMO, Moscow (2007), pp. 264–269.

43. A. M. Oleksiychuk and R. V. Proskurovskyi, “Estimation of the average error probability of the Bayesian criterion for testing hypotheses in the problem of cryptanalysis of a combining gamma generator with nonuniform movement,” Teor. Imovirn. Mat. Stat., No. 78, 152–159 (2008).

44. A. N. Alekseychuk, “Optimal balanced mappings in constructions of gamma generators with nonuniform movement of shift registers and protocols of transmission of keys along a tapped communication channel,” Registration, Storage, and Processing of Data, **10**, No. 4, 47–56 (2008).

45. V. A. Ivanov, “On a method of random coding,” Diskret. Mat., **11**, No. 3, 99–108 (1999).

46. A. N. Alekseychuk, “Random coding in a communication channel with additive noise distributed over a finite Abelian group,” Zakhyst Informatsii, No. 3, 7–16 (2002).

47. A. N. Alekseychuk, “Optimal random coding of equiprobable messages in a *q*-ary symmetric channel,” Zakhyst Informatsii, No. 4, 49–58 (2002).

48. L. Zavadskaya, A. Mellit, and A. Fal’, “On methods of cryptanalysis of stream ciphers,” in: Proc. 6th Intern. Sci.-Pract. Conf. “Information Security in Informational-Telecommunication Systems,” Kyiv (2003), p. 55.

49. A. N. Alekseychuk and L. V. Kovalchuk, “Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m,” Theory of Stochastic Processes, **12 (28)**, Nos. 1–2, 20–32 (2006).

50. L. V. Koval’chuk, “Upper estimates for average probabilities of differential approximations of Boolean mappings,” in: Proc. Intern. Sci. Conf. on Security and Counteraction to Terrorism (Intellectual Center of MGU, November 2–3, 2005), MTsNMO, Moscow (2006), pp. 163–167.

51. L. V. Skrypnik and L. V. Koval’chuk, “Upper bounds for average probabilities of differentials of Boolean mappings,” Zakhyst Informatsii, No. 3, 7–12 (2006).

52. A. N. Alekseychuk, “Upper bounds for parameters describing the resistance of non-Markov block ciphers to differential and linear cryptanalysis methods,” Zakhyst Informatsii, No. 3, 20–28 (2006).

53. L. V. Koval’chuk, “Generalized Markov ciphers: Construction of an estimate of practical resistance to differential cryptanalysis,” in: Proc. MGU Conf. “Mathematics and Security of Information Technologies,” MTsNMO, Moscow (2007), pp. 595–599.

54. A. M. Alekseychuk, L. V. Koval’chuk, and S. V. Pal’chenko, “Cryptographic parameters of replacement units describing the resistance of GOST-like block ciphers to linear and differential cryptanalysis methods,” Zakhyst Informatsii, No. 2, 12–23 (2007).

55. A. N. Alekseychuk, L. V. Koval’chuk, E. V. Skrynnik, and A. S. Shevtsov, “Estimates of practical resistance of the block cipher Kalina against differential linear cryptanalysis methods and algebraic attacks based on homomorphisms,” Prikladn. Radioelektronika, **7**, No. 3, 203–209 (2008).

56. A. N. Alekseychuk and A. S. Shevtsov, “Indices and estimates of resistance of block ciphers against first-order statistical attacks,” Registration, Storage, and processing of data, **8**, No. 4, 53–63 (2006).

57. S. Vaudenay, “Decorrelation: A theory for block cipher security,” J. Cryptology, **16**, No. 4, 249–286 (2003).

58. L. Koval’chuk and S. Pal’chenko, “Upper estimates for probabilities of generalized differentials of round transformations of GOST-like ciphers,” in: Proc. XIIth Intern. Sci.-Pract. Conf. “Information Security in Informational-Telecommunication Systems,” ChP “EKMO” and NITs “Tezis” of NTUU “KPI,” Kiev (2009), pp. 22–23.

59. S. V. Yakovlev, “Investigation of quality criteria and development of an algorithm for generation of long-term key elements of the encoder GOST 28147–89,” in: Proc. IVth All-Ukrainian Sci.-Pract. Conf. of Students, Graduate Students, and Young Scientists “Information Security Technologies,” Kyiv (2006), p. 34.

60. S. V. Yakovlev, “Balanced quality criteria of long-term key elements of the GOST 28147–89 data encipherment algorithm,” Inform. Tekhologii and Comp. Inzheneriya, No 1, 51–58 (2009).

61. S. V. Yakovlev, “The Feistel cascade scheme and its resistance to differential and linear analysis,” in: Legal, Normative, and Metrological Support of the Information Protection System in Ukraine, No. 1 (18), Kyiv (2009), pp. 103–108.

62. A. V. Fesenko, “Analysis of a public-key cryptosystem whose key is based on a piecewise linear image,” in: Proc. Xth Ann. Intern. Sci.-Pract. Conf. “Information Security in Informational-Telecommunication Systems,” ChP “EKMO” and NITs “Tezis” of NTUU “KPI,” Kiev (2007), pp. 32–33.

63. A. V. Fesenko, “Construction of a keyless attack on a cryptosystem based on a piecewise-linear mapping,” Probl. Upravlen. Inf., No. 5, 149–156 (2008).

64. A. V. Fesenko, “Construction of a keyless attack on a cryptosystem based on a piecewise linear mapping,” Probl. Upravlen. Inf., No. 1, 130–142 (2009).

65. M. M. Savchuk and A. V. Fesenko, “Investigations of the possibility of using symmetric ciphers for construction of postquantum cryptographic protocols,” in: Proc. 6th Intern. Conf. “INTERNET–EDUCATION–SCIENCE–2008,” Vol. 2, UNIVERSUM–Vinnytsya, Vinnytsya (2008), pp. 411–412.

66. M. M. Savchuk and A. V. Fesenko, “Symmetric commutative and locally-commutative ciphers for construction of classical and postquantum protocols,” Inform. Tekhnologii ta Komp’yutern. Inzheneriya, No. 2 (12), 43–51 (2008).

67. M. N. Savchuk and V. G. Sharapov, “Analysis of a method for testing random sequences that is based on context simulation,” Legal, Normative, and Metrological Support of the Information Protection System in Ukraine, No. 1(16), 82–89 (2008).

68. M. N. Savchuk and V. G. Sharapov, “A multidimensional statistical test for binary sequences,” Legal, Normative, and Metrological Support of the Information Protection System in Ukraine, No. 1 (18), 65–72 (2009).

69. A. Anisimov, T. Avanesov, V. Tkachenko, and O. Fal’ (translation and sci.-techn. editing), DSTU ISO/IEC 18014–1:2006. Information Technologies. Protection Methods. Timestamping Service. Part 1. Fundamentals (DSTU ISO/IEC 18014–2:2002.IDT), Derzhspozhivstandart Ukrainy, Kyiv (2008).
70. A. Anisimov, T. Avanesov, V. Tkachenko, and O. Fal’, DSTU ISO/IEC 18014–2:2006. Information Technologies. Protection Methods. Timestamping Service. Part 2. Mechanisms Producing Connected Tokens (DSTU ISO/IEC 18014–2:2002.IDT), Derzhspozhivstandart Ukrainy, Kyiv (2008).
71. A. Anisimov, T. Avanesov, V. Tkachenko, and O. Fal’, DSTU ISO/IEC 18014–3:2006. Information Technologies. Protection Methods. Timestamping Service. Part 3. Mechanisms Producing Connected Tokens (DSTU ISO/IEC 18014–3:2002.IDT), Derzhspozhivstandart Ukrainy, Kyiv (2008).
72. A. A. Kostin, N. A. Moldovyan, and A. M. Fal’, “On a realization of blind signature and collective signature protocols on the basis of digital signature standards,” in: Proc. VIth Intern. Conf. “Information Security of Russia (IBRR–2009),” SPOISU, St.-Petersburg (2009), p. 111.
73. National Standard of Ukraine. Information Technologies. Cryptographic Information Protection. Digital Signature Based on Elliptic Curves. Formation and Checking. DSTU 4145–2002. State Committee of Ukraine for Technical Regulation and Consumer Policy, Kyiv (2003).
74. A. A. Levitskaya, “Invariance theorems for a class of systems of random nonlinear equations over an arbitrary finite ring with left unity,” Cybernetics and Systems Analysis, No. 6, 884–891 (2008).
75. A. N. Alekseychuk and A. S. Shevtsov, “Upper estimates of imbalance of bilinear approximations for round functions of block ciphers,” Cybernetics and Systems Analysis, No. 3, 378–387 (2010).
76. P. A. Endovitskii, “Refining the asymptotic approximation of the group size in the birthday paradox,” Cybernetics and Systems Analysis, No. 3, 518–522 (2010).
77. A. A. Levitskaya, “Solving the problem of invariance of probabilistic characteristics for a priory solvable systems of random nonlinear equations over a finite commutative ring with unity,” Cybernetics and Systems Analysis, No. 3, 365–377 (2010).