АННОТАЦИИ ДОКЛАДОВ

SECTION 1

Abornev A. V. **DIGIT-INJECTIVE TRANSFORMATIONS OF A MODULE OVER A GALOIS RING.** New classes of nonlinear permutations that can be represented by linear transformations of a module over a Galois ring are constructed.
Keywords: *digit-injective matrix, DI-matrix, permutation, Galois ring.*

Bondarenko L. N. **PROPERTIES OF STATISTICS VAR ON GROUP OF PERMUTATIONS.** Some properties of statistics var defining the number of various symbols in a word obtained by component addition mod n of permutation of degree n with a fixed permutation (a key) are considered.
Keywords: *permutation, statistics, generating polynomial, permanent, circulant.*

Bylkov D. N. **THE SECOND COORDINATE SEQUENCE OF A LINEAR RECURRENCE OF MAXIMUM PERIOD OVER RING $\mathbb{Z}_8$.** The analytical structure of the second coordinate in a linear recurrence sequence over ring $\mathbb{Z}_8$ is described. The lower bound of its rank (linear complexity) is specified. The class of polynomials and recurrences of the maximum period with the highest possible rank is found.
Keywords: *linear recurring sequence, coordinate sequence, rank, analytical structure.*

Volgin A. V. **AN IMPROVED ESTIMATE FOR THE CONVERGENCE RATE IN THE MULTIDIMENSIONAL CENTRAL LIMIT THEOREM.** An improvement is offered for the estimate of the convergence rate in the multidimensional central limit theorem. The value of the offered estimate obviously depends on the dimension of the random vectors.
Keywords: *multidimensional central limit theorem, rate of convergence, locally dependent random vectors.*

Geut Kr. L., Titov S. S. **ON POLYQUADRATIC EXTENSION OF BINARY FIELDS.** The paper is devoted to generation of irreducible polynomials of degree 2^n by using polyquadratic field extension of GF(2). Full binary tree of these polynomials is constructed. Some properties of such extension are formulated.
Keywords: *irreducible polynomial, polyquadratic extension, the trace of polynomial.*

Zaets M. V. **CLASSES OF POLYNOMIAL AND VARIATIVE COORDINATE POLYNOMIAL FUNCTIONS OVER GALOIS RING.** A new class of functions over Galois ring $R = \mathrm{GR}(q^m, p^m)$ named functions with the variative coordinate polynomiality (VCP-functions) is introduced. The relation between this class and the class of polynomial functions over R is considered. An upper bound for the amount of such functions is presented, and sufficient conditions for a VCP-function not to be a polynomial are given.
Keywords: *polynomial functions, Galois ring, coordinate set, VCP-functions.*

Kolomeec N. A. **AN AFFINE PROPERTY OF BOOLEAN FUNCTIONS ON SUBSPACES AND THEIR SHIFTS.** Let a Boolean function in n variables be affine on an affine subspace of dimension $\lceil n/2 \rceil$ if and only if f is affine on any its shift. It is proved that algebraic degree of f can be more than 2 only if there is no affine subspace of

dimension $\lceil n/2 \rceil$ that f is affine on it.
Keywords: *Boolean functions, bent functions, quadratic functions.*

Kurganskyy O. M. **ON ALGORITHMIC AND TOPOLOGICAL PROPERTIES OF ORBITS FOR PIECEWISE-AFFINE MAPPINGS.** The open reachability problem for one dimensional piecewise-affine mappings with two intervals (2-PAM) is considered. Some decidability results following from the specific topological properties of reachable states of the 2-PAM's are given.
Keywords: *piecewise-affine mapping, reachability problem.*

Mironenko O. L. **STATISTICAL INDEPENDENCE OF GENERAL SUPERPOSITION OF BOOLEAN FUNCTIONS.** The sufficient conditions are proved for a superposition of some Boolean functions to be statistically independent on the subset of variables.
Keywords: *Boolean functions superposition, statistical independence.*

Filyuzin S. Y. **ALGEBRAIC IMMUNITY UPPER BOUND FOR SOME DILLON'S BENT FUNCTIONS.** An upper bound for the algebraic immunity of some Dillon's bent functions is obtained. It is shown that for $k = 2, 3, \ldots, 8$ the degree for Tu and Deng's function in 2^k variables used in the Dillon's method for constructing bent functions of the maximum algebraic immunity equals $k - 1$.
Keywords: *Boolean function, nonlinearity, bent function, algebraic immunity.*

Fomichev V. M. **EQUIVALENCE OF PRIMITIVE SETS.** Equivalence of primitive sets of natural numbers is investigated in connection with the diophantine Frobenius problem. The equivalence is used to simplify calculations of Frobenius number $g(a_1, \ldots, a_k)$ and all numbers that are not contained in the additive semigroup generated by the set $\{a_1, \ldots, a_k\}$.
Keywords: *Frobenius's function, primitive set, additive semigroups of numbers.*

Frolova A. A. **AN ITERATIVE CONSTRUCTION OF ALMOST PERFECT NONLINEAR FUNCTIONS.** Vectorial Boolean functions F and G are equivalent if $\forall a \neq 0\, \forall b\, [\exists x(F(x) \oplus F(x \oplus a) = b) \Leftrightarrow \exists x(G(x) \oplus G(x \oplus a) = b)]$. It is proved that every class of equivalent almost perfect nonlinear (APN) functions in n variables contains 2^{2n} different functions. An iterative procedure is proposed for constructing APN functions in $n + 1$ variables from two APN and two Boolean functions in n variables satisfying some conditions. Computer experiment show that among functions in small variables there are many functions satisfying these conditions.
Keywords: *vectorial Boolean function, APN function, γ-equivalence, iterative construction.*

Cheremushkin A. V. **ON A NONLINEARITY DEGREE DEFINITION FOR A DISCRETE FUNCTION ON A CYCLIC GROUP.** An additive approach is proposed to the definition of the nonlinearity degree of a discrete function on a cyclic group. For elementary abelian groups, this notion is equivalent to ordinary "multiplicative" one. For polynomial functions on a ring of integers mod p^n, this notion is equivalent to minimal degree of a polynomial. It is shown that the nonlinearity degree is a finite number if and only if the order of the group is a power of a prime. An upper bound for the nonlinearity degree of functions on a cyclic group of order p^n is given.
Keywords: *nonlinearity degree, discrete functions.*

Sholomov L. A. **AN ECONOMICAL REPRESENTATION OF UNDERDETERMINED DATA AND SUPERIMPOSED CODES.** For underdetermined data, economical representations making it possible to reconstruct the initial data are proposed. A connection between representations and superimposed codes is found, and bounds for representations length are obtained.
Keywords: *underdetermined data representation, superimposed code, cover-free matrix.*

SECTION 2

Vitkup V. A. **ON THE REPRESENTATION OF S-BOXES IN BLOCK CIPHERS.** A known method of S-boxes partition applied against side-channel attacks is considered. Nowadays, necessary partitions are found for all the affine equivalence classes except one. In the paper, it is proved that S-boxes of this class do not have admissible partition.
Keywords: *S-box, vectorial Boolean function, affine equivalence.*

Kaluzhin A. K., Chizhov I. V. **ALGORITHM FOR RECOVERING PLAINTEXT FROM CIPHERTEXT IN MCELIECE CRYPTOSYSTEM.** An attack on McEiece cryptosystem is considered. In it a plaintext is recovered from a ciphertext by solving the encryption equation. The solution is get in two steps: finding the error vector and solving the system of linear equations. For finding the error vector, the Bernstein — Lange — Peters's algorithm is used together with some optimization techniques. The complexity of the offered attack on the cryptosystem based on Goppa (1024, 524, 50)-code equals $2^{60,1}$ bit operations that is 27,5 % less than by means of Bernstein — Lange — Peters's algorithm itself.
Keywords: *McEliece's cryptosystem, nonstructural attacks, Bernstein — Lange — Peters's algorithm.*

Karpunin G. A. **ON PROBABILITY CHARACTERISTICS OF RANDOM GRAPHS GENERATED BY ALGORITHMS FOR FINDING HASH FUNCTION COLLISIONS.** In the paper, a graph model of some algorithms for finding SHA-1 and RIPEMD collisions is described, and under the described model, an exact formula for calculating average complexity of these algorithms is given.
Keywords: *cryptographic hash functions, collisions, random graphs.*

Katerinskiy D. A. **ABOUT INVERTIBILITY FINITE AUTOMATA WITH FINITE DELAY.** Experimental estimates are obtained for the proportion of invertible, weakly invertible and strong invertible finite automata with finite delay. The estimates show that the proportion of the invertible automata is small (about 3 %) for automata with near numbers of states and output symbols and is large (over 80 %) for automata with the number of output symbols being 4 times more than the number of input symbols and 2 times more than the number of states.
Keywords: *finite automata, weakly invertibility, invertibility, analysis of invertibility, synthesis of inverse automata, proportion of invertible automata.*

Kovalev D. S. **FPGA IMPLEMENTATION OF FAPKC SYMMETRIC EQUIVALENT.** FPGA implementation of the FAPKC symmetric equivalent (called FASKC) is presented. The throughput/area comparison of the FASKC with the other finite automata cryptosystems is made. The FPGA implementation comparison of the FASKC, AES and other contemporary block ciphers is given.

Keywords: *non-linear automaton, invertible with delay automaton, finite automata cryptosystem, FAPKC, FASKC, PLD, FPGA, VHDL.*

Koreneva A. M. **BLOCK CIPHERS BASED ON TWO FEEDBACK SHIFT REGISTERS.** The conditions of providing bijectivity and involutivity properties are obtained for the block encryption algorithms which are based on a shift register with two feedbacks over the space of binary vectors. An example of a block encryption algorithm of this kind is constructed. The algorithm is based on a shift register of length 4.
Keywords: *bijectivity, iterative symmetric block ciphers, involutivity of encryption algorithm, shift registers*

Medvedev N. V., Titov S. S. **CONSTRUCTIONS OF IDEAL SECRET SHARING SCHEMES.** Linear homogeneous ideal secret sharing schemes are considered. The construction of such schemes is given over any field $\mathrm{GF}(q)$. By adding participants it is shown that such schemes are reduced to schemes on projective spaces.
Keywords: *homogeneous secret sharing schemes, matroids, Reed — Muller code*

Medvedeva N. V., Titov S. S. **ON NON-MINIMAL PERFECT CIPHERS.** An analogue of Shannon's theorem is proved for non-endomorphic ciphers.
Keywords: *perfect ciphers, non-endomorphic ciphers, maximal ciphers, non-minimal ciphers.*

Pestunov A. I. **ON RELATIONS BETWEEN THE BASIC NOTIONS OF DIFFERENTIAL CRYPTANALYSIS.** Some problems and inconsistencies in terminology related to the differential cryptanalysis of iterative block ciphers are considered. A set of definitions is suggested to solve these problems and to form a system of unified notions with no contradictions. By using the suggested definitions it is shown that the truncated characteristic is the most general notion: differential, truncated differential and characteristic are in fact particular cases of the truncated characteristic.
Keywords: *terminology, differential cryptanalysis, block cipher, characteristic.*

Chizhov I. V., Borodin M. A. **THE FAILURE OF MCELIECE PKC BASED ON REED — MULLER CODES.** This paper describes new algorithm for breaking McEliece cryptosystem, being built on Reed — Muller binary code $RM(r, m)$.The algorithm calculates the private key from the public key using $\mathrm{O}(n^d + n^4 \log_2 n)$ bit operations, where $n = 2^m, d = (r, m-1)$. In case of limited d, the attack has a polynomial complexity. Practical results of implementation show that McEliece cryptosystems, based on the Reed — Muller binary code of length $n = 65526$ bits, can be broken in less than 7 hours on a personal computer.
Keywords: *McEliece cryptosystem, Reed — Muller code, polynomial attack.*

SECTION 3

Alekhina M. A., Barsukova O. U. **ABOUT UNRELIABILITY BOUNDS FOR CIRCUIT WITH INVERSE FAULTS AND FUNCTIONAL ELEMENT BREAKDOWNS.** The realization of Boolean functions by circuits of unreliable functional elements is considered in an arbitrary complete basis. It's supposed that all circuit elements are independently of each other proned to faults of two types: output inverse faults and element breakdowns. Upper and lower asymptotical bounds of circuit unreliability are presented.
Keywords: *Boolean functions, functional element, circuit, unreliability of circuit, output inverse faults, element breakdowns.*

Anisenya N. I., Stefantsov D. A., Torgaeva T. A. **THE BLACKBOX SERVICE FOR HOSTING CAPTURE THE FLAG COMPUTER SECURITY COMPETITIONS.** The BlackBox system developed by the Tomsk State University team SiBears for hosting the task-based Capture the Flag competitions in computer security is introduced. The functionality of the system is described along with the peculiarities of its development and administration. The proposals about the future development are made.
Keywords: *SiBears, BlackBox, CTF.*

Vasin A. V. **ABOUT BASISES WHOSE UNRELIABILITY COEFFICIENT EQUALS 1.** Circuits composed of unreliable functional elements in a complete finite basis B are considered. It is assumed that all elements are independently of each other subjected to inverse failures at the outputs with the probability ε ($\varepsilon \in (0, 1/2)$). In the paper, a set G of Boolean functions is found, and it is proved that if $B \cap G \neq \varnothing$, then almost all Boolean functions are realized in basis B by asymptotically optimal on reliability circuits with unreliability ε under $\varepsilon \to 0$.
Keywords: *unreliable functional gates, circuits asymptotically optimal with respect to reliability, inverse failures on outputs of gates.*

Devyanin P. N. **CORRECTNESS OF STATE TRANSFORMATION RULES IN MROSL DP-MODEL.** Conditions and results of application are analysed for state transformation rules in mandatory entity-role security model of access and information flows control in OS of Linux set (MROSL DP-model). The correctness of the rules is considered with regard to requirements of mandatory access control (MAC), mandatory integrity control (MIC) and role-based access control (RBAC).
Keywords: *computer security, formal model, access control.*

Zaytsev G. Yu., Potapkin A. I., Stefantsov D. A. **MODIFICATION OF COMPILED APPLICATIONS FOR THE ANDROID PLATFORM BY MEANS OF ASPECT-ORIENTED PROGRAMMING.** The tool for modification of compiled applications for the Android platform by means of aspect-oriented programming is presented. It is based on the Aspect-Oriented Programming paradigm, is implemented with the ASMDEX library, and performs the weaving of the program and the aspects in two passes. The language for implementation of the aspects is Java with special annotations encapsulating the necessary meta-information.
Keywords: *aspect-oriented programming, Android, Dalvik.*

Kolegov D. N., Tkachenko N. O., Chernov D. V. **DEVELOPMENT AND IMPLEMENTATION OF MANDATORY ACCESS CONTROL MECHANISMS IN DBMS MYSQL.** The paper is devoted to development and implementation of mandatory access control mechanisms for DBMS MySQL based on discretionary access policy. A formal security model is proposed for multilevel security mandatory access policy. It is implemented in MySQL core reference monitor enabling to protect DBMS against prohibited information and match security requirements for trusted computer systems.
Keywords: *computer security, access control, information flows, formal security model.*

Shcherba E. V., Volkov D. A. **DEVELOPMENT OF A DDOS-ATTACK DETECTION SYSTEM USING QUEUING THEORY.** A specialized system architecture is proposed for DDoS attack detection. It is based on the evaluation of the packet loss probability and the theory of queuing networks.
Keywords: *network attacks detection, denial of service, DDoS.*

SECTION 4

Abrosimov M. B., Modenova O. V. **ABOUT THE LOWER BOUNDS FOR THE NUMBER OF ADDITIONAL ARCS IN A MINIMAL VERTEX 1-EXTENSION OF ORIENTED PATH.** A graph G^* with $n + k$ vertices is vertex k-extension of a graph G if every graph obtained by removing any k vertices from G^* contains G; it is called minimal vertex k-extension of G if it has the least number of arcs among all vertex k-extensions of graph G with $n + k$ vertices. A lower bound for the number of additional arcs in minimal vertex 1-extension of an oriented path is given.
Keywords: *graph, minimal vertex extension, fault tolerance.*

Batueva T. **PROPERTIES OF GENE NETWORKS WITH THRESHOLD FUNCTIONS.** An algorithm for finding all fixed points of the state graph of a circulant type gene network transformed by a Boolean function is given. All sources of the state graph of a gene network transformed by a threshold Boolean function in k variables with a single value 1 are described. In case $k = 3$ all circles of the state graph are described too, and the length of the maximum chain in it is calculated.
Keywords: *gene network, directed graph, threshold functions, state graph of mapping, fixed point, source of state graph.*

Bondarenko P. P. **ON THE UPPER BOUND FOR THE NUMBER OF ADDITIONAL EDGES IN MINIMAL VERTEX EXTENSIONS OF COLORED CIRCLES.** An upper bound for the number of additional edges in the minimum vertex 1-extensions of cycles with the vertices of two types and a general construction of one of such extensions are given.
Keywords: *graph, circle, minimal extension, fault-tolerance.*

Evdokimov A. A., Kochemazov S. E., Otpushennikov I. V., Semenov A. A. **DYNAMICAL PROPERTIES OF SOME DISCRETE AUTOMATON MAPPINGS DEFINED BY RANDOM GRAPHS.** In this report, the results of computational analysis are presented for problems of searching fixed points and cycles of some discrete mappings, that are used to model the behaviour of systems with many interconnecting agents and are defined by random graphs generated according to known models (G_{np}-graphs, the Watts — Strogatz model).
Keywords: *random graphs, gene networks, discrete automaton mappings, SAT.*

Zharkova A. V. **ON BRANCHING AND IMMEDIATE PREDECESSORS OF THE STATES IN FINITE DYNAMIC SYSTEM OF ALL POSSIBLE ORIENTATIONS OF A GRAPH.** Branching and immediate predecessors of the states in the finite dynamic system of all possible orientations of a given graph are found. Evolutionary function of the system transforms digraphs by reorientation of all arcs entering the sinks. The inaccessibility property is defined for a state in this dynamic system.
Keywords: *finite dynamic system, graph, graph orientation, branching, inaccessibility, immediate predecessor.*

Komarov D. D. **MINIMAL EDGE EXTENSIONS OF SPECIAL TYPE PALM TREES.** Minimal edge 1-extensions of 2-leaf palm trees are described.
Keywords: *extensions of graphs,palm trees.*

Kornienko A. S. **FUNCTIONAL GRAPH TREES FOR CIRCULANTS WITH LINEAR BOOLEAN FUNCTIONS AT THE VERTICES.** The functional graph of a discrete dynamic system being a model of regulatory gene network circuit is de-

fined as the graph of the transformation $A_{f,2} : F_2^n \to F_2^n$ where $A_{f,2}(v_0, v_1, \ldots, v_{n-1}) = (u_0, u_1, \ldots, u_{n-1})$, $u_i = v_{i-1} + v_i + v_{i+1}$, $i = 0, 1, \ldots, n-1$, $v_{-1} = v_{n-1}$, $v_n = v_0$. The structure of this graph is completely described.
Keywords: *discrete dynamical system, circulant, gene network, regulatory circuit, functional graph.*

Kyazhin S. N. **ON LOCAL PRIMITIVENESS OF GRAPHS AND NONNEGATIVE MATRICES.** Cryptographic generators constructed of control and generating blocks are investigated. Essential dependence of block elements on all signs of generator initial state is the useful property of such generators. The notion of a local primitiveness for a nonnegative matrix or graph is introduced to study such dependences. The conditions for matrix local primitiveness are obtained. A relation between the local primitiveness characteristics of matrices (graphs) of particular classes and parameters of generators is established.
Keywords: *exponent, local exponent, primitive matrix, primitive graph, local primitiveness.*

Nazhmidenova A. M. **THE DISCRETE DYNAMIC SYSTEM ON A DOUBLE CIRCULANT WITH DIFFERENT FUNCTIONS AT THE VERTICES.** The structure of the functional graph is studied for a discrete dynamic system consisting of two circulants $G_{n,k}$ with different orientations and functionings and with the corresponding vertices being conjugate. The recurrent relation for the number of fixed points is obtained, and the asymptotic behaviour of this number is described. In the case $k = 2$ the theorems characterizing structural properties, fixed points, pendant vertices and cycles of length 2 of the functional graphs are proved. In particular, the explicit formulas for the number of fixed points and pendant vertices are found.
Keywords: *gene network, discrete model, regulatory loop, circulant, functional graph, cycles, fixed points, pendant vertices.*

Osipov D. U. **ON T-IRREDUCIBLE EXTENSIONS OF STARLIKE TREES.** T-irreducible extension is a kind of the optimal extension of a graph. In the paper, all nonisomorphic T-irreducible extensions are constructed for starlike trees with paths of one and the same length.
Keywords: *graph, T-irreducible extension, starlike trees.*

Salii V. N. **ON THE ORDERED SET OF CONNECTED PARTS OF A POLYGONAL GRAPH.** Polygonal graphs, whose the ordered set of abstract connected parts is a lattice, are characterized.
Keywords: *polygonal graph, linear graph, binary vector, duality, ordered set, lattice.*

Tokareva N. N. **SIMPLE PROOF FOR THE STRONG REGULARITY OF THE CAYLEY GRAPH OF BENT FUNCTION.** A simple proof is presented for the known result about the strong regularity of Cayley graph of a bent function.
Keywords: *bent functions, strongly regular graphs.*

Tsitsiashvili G. Sh., Osipova M. A., Losev A. S. **ASYMPTOTICS OF CONNECTIVITY PROBABILITIES FOR PAIRS OF GRAPH NODES.** For graphs with low reliable arcs, asymptotics of probabilities for connectivities between all pairs of nodes are constructed. Parameters of these asymptotics are characteristics of shortest paths in the graph. To calculate these characteristics, some modifications of classical algorithms are developed. On the base of these results, numerical experiment is realized. This experiment

demonstrates advantages of suggested algorithms.
Keywords: *shortest path, connectivity probability, computational complexity.*

SECTION 5

Агибалов Г. П., Липский В. Б., Панкратова И. А. **КРИПТОГРАФИЧЕСКОЕ РАСШИРЕНИЕ РУССКОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ.** Представлено расширение русского языка программирования ЛЯПАС, получившее название ЛЯПАС-Т и заключающееся в увеличении длины операндов и расширении множества элементарных операций над ними. Необходимость в нём продиктована, в первую очередь, потребностями страны в доверенных и эффективных программной и аппаратной реализациях современных криптографических алгоритмов в безопасных компьютерных системах логического управления критически важными объектами, такими, как космические системы, энергетические установки, ядерное оружие, подводные лодки, беспилотники и т. п. Представлен также компилятор ЛЯПАСа-Т, генерирующий его загрузочный модуль для операционной системы Linux.

Ключевые слова: *русский язык программирования, криптографическое расширение, ЛЯПАС-Т, компилятор.*

Агибалов Г. П., Липский В. Б., Панкратова И. А. **ПРОЕКТ АППАРАТНОЙ РЕАЛИЗАЦИИ РУССКОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ.** Представлен проект процессора, реализующего ЛЯПАС-Т аппаратно, и предпроцессора, конвертирующего программы на ЛЯПАСе-Т в исполняемый код процессора. Сообщается о процессоре для подмножества ЛЯПАСа-Т без подпрограмм, операций над комплексами и длинных операндов, описанном на VHDL, протестированном средствами компьютерного моделирования и реализованном на ПЛИС с помощью системы автоматизированного проектирования.

Ключевые слова: *русский язык программирования, ЛЯПАС-Т, аппаратная реализация, предпроцессор.*

Брославский О. В. **AES НА ЛЯПАСЕ.** Представлены программы на языке ЛЯПАС, реализующие симметричный блочный алгоритм шифрования AES и расширение ключа для него.

Ключевые слова: *AES, ЛЯПАС.*

SECTION 6

Anashkina N. V. **ABOUT POSSIBILITY OF REDUCTION OF SORT OUT IN BALASH'S ALGORITHM.** An optimization of Balash's algorithm using particular feature of geometric structure of deadlock point's environs is presented.
Keywords: *Balash's algorithm, discrepancy, deadlock point.*

Arbuzov D. S., Tuktarova L. I. **ANALYSIS OF SOME ALGORITHMS FOR SMOOTH INTEGERS RECOGNITION.** The experimental comparison of three sieving algorithms by run time and memory amount is presented.
Keywords: *smooth numbers, sieving, Bernstein algorithm.*

Bulavintsev V. G., Semenov A. A. **GPU-BASED IMPLEMENTATION OF DPLL ALGORITHM WITH LIMITED NON-CHRONOLOGICAL BACKTRACKING.** A new GPU-based SAT solver named ngsat is presented. The solver employs DPLL

algorithm with limited version of non-chronological backtracking without Clause Learning. Some new techniques are developed and applied to increase the effectiveness of DPLL algorithm on SIMD. Ngsat's performance is demonstrated in application to the problems of search for pairs of orthogonal Latin squares.
Keywords: *GPU, DPLL algorithm, SAT, parallel computer architectures, CUDA, SIMD.*

Bykova V. V. **ASYMPTOTIC SOLUTION OF THE RECURRENCE RELATIONS IN THE ANALYSIS OF SPLITTING ALGORITHMS FOR SAT.** The traditional technique for analysis of splitting algorithms for SAT problem is considered. A theorem establishing the upper bounds for execution time of algorithms in the case of balanced splitting is offered.
Keywords: *splitting algorithms, computational complexity.*

Zhukov K. D., Rybakov A. S. **ON SOLVING BIG SYSTEMS OF CONGRUENCES.** Let S be a finite set of positive integers such that almost all its elements are pairwise coprime. An algorithm is presented for finding all elements $s \in S$, such that $(s, s') > 1$ for an element $s' \in S$, $s' \neq s$. The algorithm allows to reduce any system of polynomial congruences to a number of systems with coprime moduli.
Keywords: *coprime base, gcd, merge gcd, gcd tree.*

Klimina A. S. **OPTIMIZATION OF POLLARD'S $(p-1)$-ALGORITHM.** The article contains criteria for choice of parameters and a method for optimization of the Pollard's $(p-1)$-algorithm.
Keywords: *Pollard's $(p-1)$-algorithm, integer factorization.*

Kuznetsova A. S., Kuznetsov A. A., Safonov K. V. **A PARALLEL ALGORITHM FOR COMPUTATION OF GROWTH FUNCTIONS IN THE FINITE TWO-GENERATOR GROUPS OF PERIOD 5.** A parallel version of the algorithm for computation of growth functions in the finite two-generator groups of period 5 is presented.
Keywords: *the growth function of the group, the Cayley diameter, a parallel algorithm.*

Pottosin Yu. V., Kardash S.N. **PIPELINING OF COMBINATIONAL CIRCUITS.** The problem is set to divide a given multilevel combinational circuit into a given number of cascades with registers providing pipeline-wise development of incoming signals. To solve this problem a model based on representation of combinational circuit in the form of digraph is used.
Keywords: *combinational circuit, pipelining, directed graph.*

Ryabokon D. V. **ALGORITHM FOR SEARCHING PROHIBITIONS OF BOOLEAN FUNCTIONS.** An algorithm for search of prohibitions of Boolean function based on the branch and bound method is proposed. It allows to find a prohibition of Boolean function, a prohibition of minimum length or all prohibitions under a specified length.
Keywords: *prohibition of Boolean function, de Bruijn graph.*

Semenov A. A. **ON THE EFFECTIVE REPRESENTATION OF DISJUNCTIVE NORMAL FORMS BY DIAGRAMS OF A SPECIAL KIND.** For an arbitrary disjunctive normal form of a Boolean function, a disjunctive diagram representation is proposed. This kind of diagrams is constructed in a polynomial time and can be used to reduce the size of conflict databases produced during non-chronological DPLL derivation.
Keywords: *decision diagrams, BDD, ZDD, disjunctive diagrams.*

Usatyuk V. S. **IMPLEMENTATION OF THE PARALLEL SHORTEST VECTOR ENUMERATION IN THE BLOCK KORKIN — ZOLOTAREV METHOD.**

A parallel CPU implementation of Kannan algorithm is presented for solving shortest vector problem in block Korkin — Zolotarev lattice reduction method. The implementation is based on Native POSIX Thread Library and shows the linear decrease of runtime with the number of threads.
Keywords: *shortest vector problem, SVP, block Korkin — Zolotarev, BKZ, lattices, parallel algorithms.*

Chernyak R. I. **PARALLELIZATION OF THE DECODING ALGORITHM IN VIDEO COMPRESSION STANDARD H.265/HEVC.** A method for parallel implementation of the decoder in the video compression standard H.265/HEVC is proposed. The effectiveness of the method is proved theoretically and shown experimentally.
Keywords: *H.265/HEVC, digital video compression, HEVC decoder parallelization.*

Shangin R. E. **EXACT ALGORITHM FOR SOLVING SPECIAL CASE OF DISCRETE WEBER PROBLEM.** An algorithm reasonably solving Weber problem for n-sequentially connected chain and finite set of points of location is described. The algorithm is compared with an integer linear programming algorithm realized in IBM ILOG CPLEX.
Keywords: *Weber problem, n-sequentially connected chain, dynamic programming, exact algorithm, quasi-polynomial algorithm.*