АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

SECTION 1

Alekseenko E. S. **AN ALGORITHM OF COMPUTING D-GAP NUMBERS AND D-WEIERSTRASS POINTS.** For a functional field associated with an algebraic curve and having any characteristic, an algorithm for computing D-gap numbers and D-Weierstrass points is described.

Evdokimov A. A. **CODING OF FINITE INTEGER LATTICE BY MEANS OF MAPPINGS WITH A BOUNDED DISTORTION.** A class of mappings with a bounded distortion for embeddings of finite integer lattice into Boolean hypercubes is considered.

Kolomeec N. A. **THE NUMBER OF BENT FUNCTIONS ON THE MINIMAL DISTANCE FROM A QUADRATIC BENT FUNCTION.** We are interested in how to construct bent functions by slight modifications of an initial one. The answer to this question is directly connected with the studying bent functions on the minimal Hamming distance from a given bent function. Here, we describe all bent functions on the minimal distance from a quadratic bent function and calculate exactly the number of them.

Kolcheva O. L., Pankratova I. A. **STATISTICAL INDEPENDENCE OF THE BOOLEAN FUNCTION SUPERPOSITION.** It is proved here that if a Boolean function $f(x, y)$ is statistically independent on the variables in x, then the same is true for any Boolean function $g(f(x, y), z)$, but this may not be so for a superposition $g(f_1(x, y), \ldots, f_s(x, y), z)$ where $s \geqslant 2$ and every function $f_1(x, y), \ldots, f_s(x, y)$ is statistically independent on x.

Korsakova E. P. **CLASSIFICATION OF ANF GRAPHS FOR QUADRATIC BENT FUNCTIONS IN 6 VARIABLES.** Classification of quadratic bent functions in 6 variables based on a new notion of graph equivalence for bent functions is suggested.

Parvatov N. G. **WEAKLY CENTRAL CLONES AND COMPLETENESS PROBLEM FOR THEM.** A weakly central clones are introduced and completeness problem for them is considered.

Pichkur A. B. **DESCRIPTION OF THE CLASS OF PERMUTATIONS, REPRESENTED AS A PRODUCT OF TWO PERMUTATIONS WITH FIXED NUMBER OF MOBILE POINTS.** The structure of the class of permutations represented as the product of two permutations with q mobile points, $4 \leqslant q \leqslant N/2$, is completely described.

Pogorelov B. A., Pudovkina M. A. **ON APPROXIMATION OF PERMUTATIONS BY IMPRIMITIVE GROUPS.** In this paper, we discuss how to find the distance between a permutation and an imprimitive group having or not a fixed system of blocks.

Potapov V. N. **ON PERFECT 2-COLORINGS OF THE Q-ARY HYPERCUBE.** A coloring of the q-ary n-dimensional cube (hypercube) is called perfect if, for every n-tuple x, the collection of the colors of the neighbors of x depends only on the color of x. A Boolean-valued function is called correlation-immune of degree $n - m$ if it takes the value 1 the same number of times for each m-dimensional face of the hypercube. Let $f = \chi^S$ be a characteristic function of some subset S of hypercube. In the paper the inequality $\rho(S)q(\mathrm{cor}(f)+1) \leqslant A(S)$ is proved, where $\mathrm{cor}(f)$ is the maximum degree of the correlation immunity of f, $A(S)$ is the average number of neighbors in the set S for n-tuples in a complement of a set S, and $\rho(S) = |S|/q^n$ is the density of the set S. Moreover, the function f is a perfect coloring if and only if we obtain an equality in the above formula.

Pryanichnikova E. A. **ALGEBRAS OF LANGUAGES ASSOCIATED WITH LABELLED GRAPHS.** In this work, we introduce a family of algebras that may serve as an effective tool for characterization of languages, that can be represented by labelled graphs, and study its properties. It is proved that the language is represented by a regular expression in considered algebras if and only if this language is associated with the labelled graph. This result is an analog of well-known Kleene's theorem for finite automata.

Tokareva N. N. **HYPOTHESES FOR THE NUMBER OF BENT FUNCTIONS.** We study bent iterative functions and their applications for the long-standing problem to find exact number of all bent functions.

SECTION 2

Abornev A. V., Bylkov D. N. **POLYNOMIALS OVER PRIMARY RESIDUE RINGS WITH A SMALL UNIQUE DISTANCE.** We consider polynomials over small residue rings. For polynomials with the unique distance equaled to twice the degree of the polynomial, we show how to use them for constructing cryptographic primitives.

Andreeva L. N. **MAPPING ENLARGEMENTS PRESERVING IDENTIFICATION PROPERTY.** Mappings defined on a Cartesian power of a finite set with the property to be identified on a subset of co-domain coordinates are considered. A mapping enlargement preserving the identification property is suggested. In the secret sharing schemes based on involutions, the result can be applied to specify authorized subsets when a new patticipant is added.

Artamonov A. V., Vasilev P. N., Makhovenko E. B. **PROVABLE SECURE DYNAMIC GROUP SIGNATURE SCHEME.** The article describes the modification of basic group signature scheme BBS for the purpose of its application for distributed systems with variable structure. The mechanism of classification and comparison for group signatures is proposed. The BBS scheme is improved according to the requirements of application area. Security of new group signature scheme is proved.

Voronin R. I. **ALGEBRAIC CRYPTANALYSIS OF ONE-ROUND S-AES.** We investigate applicability of the algebraic cryptanalysis to S-AES. We use 2 different pairs of plaintexts and ciphertexts that allow us to obtain the system with only 32 equations and 16 variables. We analyse the efficiency of such an approach.

Erofeev S. Y. **DISCRETE LOGARITHM DIOPHANTINESS.** The paper proposes a new representation of discrete logarithm in Z_p by constructing a diophantine equation, such that finding solution to this equation and finding discrete logarithm are equivalent problems.

Erofeev S. Y., Romankov V. A. **CONSTRUCTING OF ONE-WAY FUNCTIONS BASED ON UNDECIDABILITY OF THE ENDOMORPHISM PROBLEM IN GROUPS.** The paper proposes a scheme for constructing one-way function in a group with decidable word problem and undecidable endomorphism problem, and a corresponding authentication protocol. Possible prerequisites for reliability of the proposed scheme are analysed.

Kovalev D. S., Trenkaev V. N. **FPGA IMPLEMENTATION OF FINITE AUTOMATA PUBLIC KEY CRYPTOSYSTEM.** The paper presents FPGA implementation of Finite Automata Public Key Cryptosystem (FAPKC). The dependence of the throughput/hardware resources on cryptosystem parameters is investigated. FPGA implementations of FAPKC and RSA are compared.

Kukalo I. A. **ANALYSIS OF THE GOST 28147-89 MODES OF OPERATION THAT PROVIDE CONFIDENTIALITY.** In this research, the security estimation of the GOST 28147-89 modes against adaptive chosen-plaintext attack is executed. For each mode, the size of the data guaranteing preservation of the information confidentiality is defined.

Lebedeva O. N. **ON THE CHOICE OF SLID PAIRS FOR THE CORRELATION CRYPTANALYSIS OF KEELOQ.** We suggest an improvement for the correlation cryptanalysis of KeeLoq based on the filtering slid pairs.

Pudovkina M. A. **ON IMPOSSIBLE TRUNCATED DIFFERENTIALS OF XSL CIPHERS.** Impossible differential cryptanalysis is a very popular tool for analysing the security of modern block ciphers. The core of such attack is based on the existence of impossible differentials. In this paper, we generalize results obtained by R. Li, B. Sun, C. Li.

SECTION 3

Abrosimov M. B., Matorin A. A. **RELIABILITY ANALYSIS OF GRAPHICAL CAPTCHA-SYSTEMS BY THE EXAMPLE OF KCAPTCHA.** CAPTCHA constructed on the basis of distorted images is considered. Reliability of CAPTCHA image is analysed for a system KCAPTCHA. An algorithm for automated recognition of generated images is presented. The effectiveness of graphic CAPTHCHA recognition and reliability are discussed.

Devyanin P. N. **ABOUT THE ROLE DP-MODEL FOR ACCESS AND INFORMATION FLOWS CONTROL IN OPERATING SYSTEMS OF LINUX FAMILY.** Here, DP-model named in the title is presented. There are many essential features which differ it from DP-models earlier developed for other computer systems. In particular, it contains nonmonotone rules of state transformations being necessary in analysis of conditions for transferring access rights and realizing information flows in OS.

Kachanov M. A. **ROLE-BASED SECURITY MODEL OF *SELINUX* COMPUTER SYSTEM.** Security analysis problem for access and information flows control in *SELinux* computer system is solved; a role-based security model of such computer systems and techniques for applying this model in practice are suggested in this paper.

Kolegov D. N. **THE DEVELOPMENT FEUTURES OF NETWORK ACCESS CONTROL DP-MODEL.** Some features of network access control and methods for their representation in DP-model are presented here.

Kononov D. D., Isaev S. V. **THE SECURITY MODEL FOR CROSS-PLATFORM WEB SERVICES OF MUNICIPAL PROCUREMENT SUPPORT.** This article describes RBAC-based security model and its software implementation for web-based support of municipal orders (including electronic auctions) in Krasnoyarsk city administration. The work is a part of Automated System of Municipal Orders Support.

Miloshenko A. V., Solovjev T. M., Chernyak R. I., Shumskaya M. V. **DEVELOPMENT OF COMPREHENSIVE TAUGHT SYSTEM THAT PROTECTS INFORMATION RESOURCES FROM PHISHING ATTACKS.** This research is devoted to development of comprehensive taught system that protects information resources from phishing attacks. Based on thorough analysis of available phishing resources, a set of identifiers, characteristics of phishing websites, are determined. The possibility of detecting these identifiers has been studied, and corresponding algorithms have been developed. The main challenge of this research was to analyse the cumulative effect of identifiers. It was addressed during system development stage. As a result, a mechanism (based on optimization techniques) that determines the risk level of a certain website has been developed. Learning capability of the system is based on data mining. Specifically, neural network technology and linear regression methods have been used extensively. Existing phishing websites databases have been used to create a learning sample.

Proskurin V. G. **APPROACHES TO DEVELOPMENT OF DISCRETIONARY DP-MODEL OF THE MODERN SECURE OPERATING SYSTEMS.** This article represents the discretionary DP-model (ZOS DP-model) developing and concretizing existing DP-models for a case when the secure operating system (OS) is considered as modeled computer system. This new DP-model allows to apply the scientific tools of DP-models to formal description and a scientific substantiation of the various practical decisions implemented in modern secure OS. In particular, it is supposed to use ZOS DP-model for increasing the security of domestic operating systems.

SECTION 4

Bykova V. V. **FPT-ALGORITHMS AND THEIR CLASSIFICATION ON THE BASE OF ELASTICITY.** We give a brief overview of the results and problems of parameterized algorithmics as the new direction of computational complexity theory. For a parameterized algorithm, we offer a new indicator of computational complexity which can be used to measure the growth rate of its complexity function depending on many variables. This indicator is a partial elasticity of the complexity function. We offer a two-dimensional classification of parameterized algorithms with the complexity function having a multiplicative form of presentation.

Safonov K. V., Kalugin-Balashov D. A. **ABOUT PHRASE-STRUCTURE GRAMMAR PROPERTY.** A necessary condition are given for a system of symbolic equations defining the language of the phrase structure in which this language is represented as a formal non-commutative series.

Stephantsov D. A., Kryukova A. E. **A DENOTATIONAL SEMANTICS FOR THE ASPECTTALK PROGRAMMING LANGUAGE.** The denotational semantics for the aspect-oriented programming language AspectTalk is presented. It is constructed as a triple consisting of syntactic sets, semantic domains, and a set of functions from the syntactic sets into the semantic domains.

Stephantsov D. A., Tkachenko N. O., Chernov D. V., Shmakova R. V. **DESIGN AND IMPLEMENTATION OF THE ORM LIBRARY IN C++.** The Object-Relational

Mapping (ORM) library for C++ programming language is presented. Its design and implementation are discussed. The library is compared with other ORM implementations, namely ODB and Wt::Dbo, and its advantages are concerned.

SECTION 5

Zaikin O. S. **SOLVING OF CRYPTANALYSIS PROBLEMS IN GRID SYSTEMS (BY THE EXAMPLE OF BOINC).** In the paper, a technology for solving logical cryptanalysis problems in desktop grids is described. The technology was validated by successful solving of cryptanalysis problems for some keystream generators in the desktop grid based on BOINC platform.

Kolomeec N. A., Pavlov A. V. **"BOOLEAN FUNCTIONS" IS A SYSTEM FOR THE WORK WITH BOOLEAN FUNCTIONS.** This work is devoted to the new free system *Boolean Functions* designed for the work with Boolean functions, especially with bent functions. This system is oriented mainly to the programmers. It is a library of classes in C++ language. This system is available at site of Sobolev Institute of Mathematics SB RAS `http://math.nsc.ru/~bf`.

Semenov A. A., Otpuschennikov I. V., Kochemazov S. E. **APPLICATION OF SAT-APPROACH FOR SOLVING COMBINATORIAL PROBLEMS.** In the report, we present results of applying symbolic computation algorithms to solving discrete automata research problems (e.g. problems of analysis of discrete models of gene networks) and combinatorial optimization problems. In all cases, an original problem is translated into Boolean equations (and after this to SAT) and then is solved using SAT-solver. Optimization problems are solved in distributed computing environments with the help of the SAT-solver specially developed for this task.

Fomichev V. M. **ON PARALLEL COMPUTATIONS IN IMPLEMENTATION OF THE MEAT-IN-THE-MIDDLE ATTACK.** Three variants of implementations of the meat-in-the-middle attack based on clusters and distributed computations are considered for symmetric block cryptosystems. The average time of computations is estimated in universal proposition on equiprobability keys of cryptosystem. It is shown that the coefficient of curtailing for average time attains the number of processors comparing to monoprocessor system.

SECTION 6

Berezovsky Yu. V., Vorob'ev V. A. **C-MODEL OF A PREDATOR — PREY GROWTH IN THE ECOLOGICAL NICHE.** The population of automata is a model of collective behavior of automata. Modeling of population dynamics is implemented by Causal Petri Net. Net places represent the states of automata. A net marking specifies the number of automata that are in corresponding states. Transitions represent events that result from the joint actions of the elements of a population. For each transition of the net, a value is specified defining the probability (rate) of the transition response, so a system of differential equations can be built. These equations describe the dynamics of the average number of automata in places while the logical conditions specified by Petri net are implemented. The numerical solution of the system is obtained using computer simulation.

Salii V. N. **ON SKELETON AUTOMATA.** A skeleton automaton is an automaton in which the relation of mutual accessibility of states is the identity relation. We prove that automata that admit a regular enumeration of states are exactly skeleton automata. It is shown how for a given automaton one can construct an automaton with minimal number of states that has the same subautomata lattice, and is necessarily a skeleton automaton. A procedure is proposed to obtain a skeleton automaton from a given automaton by removal of minimal number of arcs in its transition diagram.

Trenkaev V. N. **FAULT ATTACK ON RECONFIGURABLE FSM-BASED CIPHER OF ZAKREVSKIJ.** The paper presents a fault attack on reconfigurable FSM-based cipher of Zakrevskij. The faulty effect is assumed to be transient. The attack is based on the single stuck-at fault model and a solution of the problem of finite-state machine identification. Simple conditional experiments with automata are used.

SECTION 7

Abrosimov M. B., Bondarenko P. P. **MINIMAL EXTENSIONS FOR CYCLES WITH VERTICES OF TWO TYPES.** For cycles with vertices of two types where one vertex is of the first type and other vertices are of another type, the minimal vertex extensions are described.

Abrosimov M. B., Dolgov A. A. **ON THE UNIQUENESS OF EXACT VERTEX EXTENSIONS.** The paper discusses the uniqueness of the exact vertex extensions of graphs. This problem is closely related to reconstruction of graphs. For undirected graphs, the uniqueness has been proved earlier. For oriented graphs, full solution is not known. The obtained result means that if there is a digraph G with the number of vertices greater than 2, which has two or more nonisomorphic 1-vertex exact extansions, the number of vertices of the digraph G is not less than 13, and exact vertex 1-extensions are not reconstructible and do not belong to any known family of nonreconstructible digraphs.

Abrosimov M. B., Komarov D. D. **ON MINIMAL EDGE 1-EXTENSIONS OF TWO SPECIAL FORM TREES.** In this paper, we consider two families of trees: one family consists of superslim trees and another one of trees that are a combination of star graphs with adjacent centers. For these families, we propose schemes for constructing one minimal edge-1-extensions.

Abrosimov M. B., Modenova O. V. **ON PROPERTIES OF MINIMAL EXTENSIONS OF ORGRAPHS.** Some properties of minimal vertex extensions of directed graphs are studied, and analysis of the results of computational experiment on the construction of minimal vertex 1-extensions of oriented graphs with the number of vertices up to 6 is given.

Bykova V. V. **COMPUTATIONAL ASPECTS OF TREEWIDTH FOR GRAPH.** A brief overview of recent results on the problem of treewidth for the graph is givev; some of the lower and upper bounds for treewidth are investigated; algorithmic methods to improve these bounds are presented.

Vlasova A. V. **ON ATTRACTORS OF DYNAMICAL SYSTEMS ASSOCIATED WITH CYCLES.** A theorem that describes attractors of dynamical systems associated with cycles is proved. States of such a system are binary vectors of a given dimension and evolutional function transforms vectors according to the following rules: if both the initial component is 0 and the final one is 1 they are replaced by 1 and 0 respectively and all digrams 10 are replaced simultaneously by 01.

Grunsky I. S., Sapunov S. V. **ON MOBILE AGENT SELF-LOCATION USING TOPOLOGICAL PROPERTIES OF ENVIRONMENT.** The paper is dedicated to methods of distinction of vertices in labeled graphs by an automaton walking on the graph and reading vertex labels. This problem arises in the navigation of mobile robots using topological maps of the environment. We propose construction and realization methods for distinguishing experiments with deterministic graphs based on checking the isomorphism of subgraphs generated by all vertices that are accessible from compared vertices.

Karmanova E. O. **ON CONGRUENCES OF PATHS.** A congruence of a path is an equivalence relation on the set of path's vertices all of whose classes are independent subsets. It is shown that each connected graph is a quotient-graph of a suitable path. Valuations are established for a minimal length of a chain whose quotient-graph is a given graph.

Kochkarov A. A., Sennikova L. I., Bolurov N. N. **ON SOME PREFRACTAL GRAPHS PROPERTIES.** This paper is devoted to some structural properties of prefractal graphs. A procedure for generating prefractal graphs is described. Upper and least bounds for the number of cutpoints and bridges in prefractal graphs are given.

Melent'ev V. A. **COMPACT GRAPHS AND THE DETERMINISTIC ALGORITHM FOR THEIR SYNTHESIS.** Compact structures of computational systems are defined as regular graphs with the minimum diameter. A method for synthesis of compact graphs using the representation of the graph by a set of its vertex-complete projections with the minimally possible number of levels is described.

Melent'ev V. A. **RESTRICTIONS ON GIRTHS IN COMPACT GRAPHS.** By definition, the compact graph is a regular graph with the minimum diameter. In the paper, the compactness conditions are investigated for regular graphs with the length of a minimum cycle restricted.

Fomichev V. M. **THE IMPROVEMENT OF EXPONENT'S ESTIMATES FOR PRIMITIVE GRAPHS.** The estimates of exponents of n-vertex primitive digraphs are improved. The digraphs considered contain two prime contours whose lengths l and λ are coprime numbers. Accessible estimates of the order $\mathrm{O}(\max\{l\lambda, f(l,\lambda,n)\})$ are obtained, where $f(l,\lambda,n)$ is a linear polynomial. Primitive digraphs whose exponents are maximal (n^2-2n+2, H. Wielandt, 1950), are described completely. The estimates of exponents of n-vertex primitive undirected graphs are improved too. In particular, the exponent of an undirected graph is no more $2n-l-1$ where l is the length of the longest cycle with odd length in graph. Primitive undirected graphs whose exponents are maximal $(2n-2)$ are described completely.