

# Table of Contents

<b>Invited Paper</b>	<b>1</b>
35 Years of Progress in Digital Magnetic Recording — Hisashi Kobayashi, Francois Dolivo, Evangelos Eleftheriou . . . . .	1
<b>Session I Information Theory</b>	<b>11</b>
Rate-distortion control in wavelet-based video ompression systems with memory restriction — Eugeny Belyaev, Andrey Turlikov and Anna Ukhanova	13
Entropy Rate Estimators with a Near-Optimal Upper Bound on Variance — Alexei Kaltchenko, Ilias Kotsireas, Nina Timofeeva, En-hui Yang . . . .	18
Compression-based methods for density estimation for time series — Boris Ryabko . . . . .	22
Using Data Compressors for Homogeneity Testing — Daniil Ryabko . . . .	27
Calculating Entropy Estimate Using Binary Decision Diagrams — Stanislav Stankovic, Jaakko Astola . . . . .	32
Experimental research of the genome structure using theoretic-informational statistical tests — N. Usotskaya, B. Ryabko . . . . .	37
Data Compression Based Method Of Revealing Hidden Information In Steganographic Systems — Michail Zhilkin, Nadegda Melentsova, Boris Ryabko . . . . .	42

<b>Session II</b>	<b>Coding Theory</b>	<b>45</b>
Low Density Concatenated Codes with Reed-Solomon Component Codes —	V.B. Afanassiev, A.A. Davydov, V.V. Zyablov . . . . .	47
On partitions of the n-cube into perfect codes — Sergey V. Avgustinovich,	Olof Heden, Faina I. Solov'eva . . . . .	52
Best Known Binary Goppa Code's Chain — Sergey Bezzateev, Natalia	Shekhunova . . . . .	56
The star trellis decoding of Reed-Solomon codes — Sergei V. Fedorenko . .		58
$Z_2Z_4$ -linear codes: rank and kernel — Cristina Fernandez and Merce Villanueva		62
Rapid coding algorithm for Low Density Codes based on Reed-Solomon	Codes over $GF(q)$ — F.V. Groshev, V.V. Zablov . . . . .	66
A Space-Time Turbo Trellis Coded scheme with Decision Aided Equalizer	for Intersymbol Interference — Kazuyuki Kaneda, Toshiyuki Shohon and	
Haruo Ogiwara . . . . .		71
Discrete Channel Decoding of LDPC Codes in Flash Memories — Alexander	Kozlov . . . . .	76
Strategies for Reed-Solomon Decoding in Channels with Soft Bit Information	— Victor Y. Krachkovsky, Jonathan J. Ashley, Clifton J. Williamson and	
German Feyh . . . . .		81
Consideration of Deterministic Interleavers for Multiple Turbo Codes —	Hide Matsuhira and Haruo Ogiwara . . . . .	88
Decoding of LDPC Codes for Burst Noise Channels — Toshiyuki Shohon,	Yukito Kago, Haruo Ogiwara . . . . .	93
Asymptotically Good Low-density Codes Based on Hamming Codes —	Stephan Stiglmayr, Victor V. Zyablov . . . . .	98
Matrix-Vector Multiplication via Erasure Decoding — Peter Trifonov . . .		104
Stage-by-stage iterative decoding of low-density parity-check codes — A. V.	Trushkin and V. V. Zyablov . . . . .	109
Asymptotically “optimal” binary low density parity check codes —	V.V.Zyablov . . . . .	112

<b>Session III</b>	<b>Communication Systems</b>	<b>115</b>
	Performance Analysis and Enhancement of an Ultra-Wideband Wpan Mac in the Presence of Noise — Sergey D. Andreev, Alexey V. Vinel . . . . .	117
	Channel Optimization for Adaptive Information Rate Schemes — Leonid Bogod, Petri Bergholm, Jarmo Makinen . . . . .	123
	Impementations of Redundansy over Short Range Wireless Communication Channels — Radka Dimitrova . . . . .	128
	Spatial multiplexing with interantenna subsymbol time delay — G.S.Evseev and I.V.Katsov . . . . .	133
	Generalized Loss Systems, Loss Networks and Computational Algorithms — Hisashi Kobayashi, Brian L. Mark . . . . .	139
	Asynchronous Orthogonal Frequency Division Multiple Random Access system performance — D.S. Osipov . . . . .	144
	Superposition BICM for Broadcast Channels — F. A. Taubin . . . . .	149
	Capacity Estimation of Centralized Reservation-Based Random Multiple- Access System — Andrey Turlikov, Alexey Vinel . . . . .	154

<b>Session IV</b>	<b>Cryptography</b>	<b>161</b>
	Design of Robust Audio Digital Watermark System — Vasilij Alekseyev, Aleksey Grudinin, Valery Korzhik . . . . .	163
	An Improvement of the VBLAST Symbol Detection Algorithm for MIMO Channels — Erdal Arıkan, Yavuz Yapıcı . . . . .	166
	Converted Transformation of the Image with the Structure Destroying — Sergey Bezzateev, Eugeniı Krouk, Michail Litvinov, Gennadiy Filatov . .	173
	Modification of McEliece’s Public-Key Cryptosystem With the Use of Operators — V.A. Davydov . . . . .	174
	Distinguishing Attacks on Stream Ciphers Using the Book Stack Test — Sergey Doroshenko, Andrey Fionov, Alexey Lubkin, Viktor Monarev, Boris Ryabko . . . . .	179
	Simple Ideal Steganographic Systems for Containers with Known Statistics — Andrey Fionov, Boris Ryabko . . . . .	184
	Equivalent schemes of stream scrambler cryptosystems — S.G.Fomitchova	189
	The Effective Attack on Reduced-Round RC6 — Victor Monarev, Alexey Lubkin . . . . .	193
	Differential Cryptanalysis of Reduced-Round MARS — Andrey Pestunov .	197
	Problems on Formation Protected Digital Images — M.B. Sergeev, A.M. Sergeev, G.P. Philatov, M.Y. Litvinov . . . . .	202

<b>Session V</b>	<b>Combinatorics</b>	<b>203</b>
On Perfect Colorings of Johnson Graph in Two Colors — Sergey V. Avgustinovich, Ivan Yu. Mogilnykh . . . . .		205
Multiple Packing in Sum-type Metric Spaces — Vladimir Blinovskiy . . . . .		209
New constructions of small complete caps in $PG(N;q)$ , $q$ even — Alexander A. Davydov, Massimo Giulietti, Stefano Marcugini, Fernanda Pambianco . . . . .		213
Fast multiplication on the elliptic curve in the field of characteristics three that is using one third of the point — Svetlana V. Lazareva, Mikhail V. Stepanov . . . . .		218
Problems in Testing in the Presence of Information Redundancy — Andrej Pietschker . . . . .		224

<b>Session VI</b>	<b>Program Systems</b>	<b>227</b>
	Baseband Processing for multiple wireless protocols on base of coarse grained reconfigurable architecture — Anton Bobkov, Alexander Redkin, Oleg Semenov . . . . .	229
	FreeBSD Mandatory Access Control Usage for Implementing Enterprise Security Policies — Kirill Bolshakov, Elena Reshetova . . . . .	234
	Modeling redundancy in a component model — Michael Golm, Artem Ozhigin	240
	Programming model of coarse-grained distributed heterogeneous architecture — Vladimir Ivanov, Yuriy Sheynin, Alexey Syschikov . . . . .	246
	DPL: Domain specific programming language and tools — Sergey Mironov, Vladimir Pavlov, Sergey Yakoushkin, Vladimir Ivanov . . . . .	251
	Information Redundancy Problems in Self-Contextualized Decision Support Systems — Alexander Smirnov, Tatiana Levashova, Michael Pashkin, Nikolai Shilov . . . . .	255

<b>Session VII</b>	<b>Computing Systems and Networks</b>	<b>261</b>
	The NIBIUM <sup>3</sup> : Braking Process Modular Model with Integrated Landing Control System — N. Bogachieva, A. Zhukov . . . . .	263
	Efficient cache management, practical considerations in case of embedded system — Sergey Boldyrev, Antti Lappetelainen . . . . .	267
	The Redundancy Phenomenon In Cybernetics, Informatics and Systemics — Mikhail B. Ignatyev . . . . .	273
	Using Smart Nodes to overcome the problems of redundant data in the processing of Situational Awareness — Rainer Kolle, Hristo Kostov, Alex Tarter . . . . .	279
	Synthesis of Continuous and Pulsed Nonlinear Control Systems — A.E. Krouk, L.A. Osipov . . . . .	283
	Reliable Packet Transmission for Sensor Networks — Evgeny Linksy, Grigory S. Evseev . . . . .	284
	Adaptive and multi-flow routing in multi-agent infotelecommunication networks — Adil Timofeev . . . . .	288
	Application of Formal Model Verification for Mission-Critical Software — Vladimir Okulevich . . . . .	292
	System and model for real-time wireless video transmission — Dmitry Aleksandrov, Vladimir Bashun, Anton Sergeev, Andrey Turlikov . . . . .	294