

**2021 XVII International
Symposium "Problems of
Redundancy in Information
and Control Systems"
(REDUNDANCY 2021)**

**Moscow, Russia
25-29 October 2021**



**IEEE Catalog Number: CFP2171R-POD
ISBN: 978-1-6654-3309-9**

**Copyright © 2021 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP2171R-POD
ISBN (Print-On-Demand):	978-1-6654-3309-9
ISBN (Online):	978-1-6654-3308-2
ISSN:	2377-6781

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

CONSTRUCTION OF A PSEUDO-RANDOM NUMBER GENERATOR WHOSE OUTPUT IS A NORMAL SEQUENCE.....	1
<i>Boris Ryabko, Viacheslav Zhuravlev</i>	
DESIGN OF CODEBOOKS OPTIMIZED FOR NONCOHERENT TRANSMISSION OVER FAST FADING CHANNEL	5
<i>Alexander B. Sergienko, Polina V. Apalina</i>	
NOVEL ORDER STATISTICS-BASED DETECTOR AND CODED MODULATION FOR A DHA FH OFDMA SYSTEM.....	11
<i>Dmitry Osipov</i>	
ON UNSOURCED RANDOM ACCESS FOR THE MIMO CHANNEL.....	17
<i>Kirill Andreev, Alexey Frolov</i>	
COMPUTER MODELING SYSTEM OF ALLOCATING AND PLANNING PROCESSES OF HETEROGENEOUS RESOURCES IN INDUSTRIAL TELECOMMUNICATION NETWORKS	22
<i>Dmitry Perepelkin, Minh Pham</i>	
ESTIMATION OF AVERAGE DELAY IN SYSTEMS WITH UNSOURCED RANDOM ACCESS AND MULTIPLE DEPARTURE	28
<i>Anna Borisovskaya, Anton Glebov, Andrey Turlikov</i>	
GATEWAY DATA ENCODING, PACKAGING AND COMPRESSION METHOD FOR HETEROGENEOUS IOT-SATELLITE NETWORK.....	34
<i>Leonid Voskov, Alexei Rolich, Gleb Bakanov, Polina Podkopaeva</i>	
DIFFERENTIAL PROPERTIES OF AUTHENTICATED ENCRYPTION MODE BASED ON UNIVERSAL HASH FUNCTION (XTSMAC)	39
<i>Alexey Nesterenko</i>	
ELIMINATING BROADBAND COVERT CHANNELS IN DSA-LIKE SIGNATURES	45
<i>Andrey Fionov, Alexandr Klevtsov</i>	
ON THE EFFICIENCY OF METAHEURISTIC OPTIMIZATION FOR ADAPTIVE IMAGE STEGANOGRAPHY IN THE DFT DOMAIN	49
<i>Anna Melman, Oleg Evsutin</i>	
ON SQUARES OF DIHEDRAL CODES.....	55
<i>Kirill Vedenev, Yury Kosolapov</i>	
APPLICATION OF ALGORITHMIC INFORMATION THEORY TO CALIBRATE TESTS OF RANDOM NUMBER GENERATORS	61
<i>Boris Ryabko</i>	
NEW CODE-BASED CRYPTOSYSTEM BASED ON BINARY IMAGE OF GENERALIZED REED-SOLOMON CODE.....	66
<i>Fedor Ivanov, Eugenii Krouk, Victor Zyablov</i>	
DEVELOPMENT OF AN INFORMATION-THEORETICAL METHOD OF ATTRIBUTION OF LITERARY TEXTS.....	70
<i>Ryabko Boris, Savina Nadezhda</i>	

GAUSSIAN ONE-ARMED BANDIT PROBLEM	74
<i>Alexander Kolmogorov</i>	
ON THE CONDITIONS OF CONVERGENCE OF THE FUNCTIONAL FROM THE SUM OF INDEPENDENT RANDOM VARIABLES TO THE FUNCTIONAL FROM THE WIENER PROCESS.....	80
<i>Alexey Los, Aleksandr Belov</i>	
SCHEMES FOR LQG CONTROL OVER GAUSSIAN CHANNELS WITH SIDE INFORMATION	85
<i>Omri Lev, Anatoly Khina</i>	
VARIATIONAL AUTOENCODERS WITH EUCLIDEAN AND HYPERBOLIC LATENT SPACES FOR POPULATION GENETICS	91
<i>Igor Bogdanov, Vladimir Shchur</i>	
AN UPPER BOUND ON THE NUMBER OF BENT FUNCTIONS.....	95
<i>Vladimir N. Potapov</i>	
ON PARALLELISMS OF $PG(5, 2)$ INVARIANT UNDER A CYCLIC SUBGROUP OF ORDER 21	97
<i>Svetlana Topalova, Stela Zhelezova</i>	
ON SPHERICAL 4-DISTANCE 7-DESIGNS	101
<i>Peter Boyvalenkov, Navid Safaei</i>	
FAST DECODING OF UNION-FREE CODES.....	106
<i>Ilya Vorobyev</i>	
GROUP TESTING WITH NON-IDENTICAL INFECTION PROBABILITIES	110
<i>Mustafa Doger, Sennur Ulukus</i>	
ON WEIGHT SPECTRUM OF LINEAR CODES.....	116
<i>Vladimir N. Potapov</i>	
BOUNDS AND GENERICITY OF SUM-RANK-METRIC CODES.....	119
<i>Cornelia Ott, Sven Puchinger, Martin Bossert</i>	
NEW COMMUNICATION MODELS AND DECODING OF MAXIMUM RANK DISTANCE CODES.....	125
<i>Wrya K. Kadir</i>	
ON TRANSFORM-DOMAIN DECODING OF GENERALIZED GABIDULIN CODES : DEDICATED TO THE MEMORY OF ERNST M. GABIDULIN (1937–2021).....	131
<i>Wenhui Li, Vladimir Sidorenko, Antonia Wachter-Zeh</i>	
ANALYSIS OF BINARY AND TERNARY MESSAGE PASSING DECODING FOR GENERALIZED LDPC CODES	137
<i>Emna Ben Yacoub, Gianluigi Liva</i>	
ABOUT USAGE OF METRICS IN DECODING OF LDPC CODES IN TWO-STATE CHANNELS WITH MEMORY	143
<i>Alina M. Veresova, Anna A. Fominykh, Andrei A. Ovchinnikov</i>	
LINEAR PROGRAMMING DECODING OF NON-LINEAR SPARSE-GRAPH CODES.....	149
<i>Gleb Balitskiy, Alexey Frolov, Pavel Rybin</i>	

DEEP NEURAL NETWORK BASED DECODING OF SHORT 5G LDPC CODES	155
<i>Kirill Andreev, Alexey Frolov, German Svistunov, Kedi Wu, Jing Liang</i>	
BIDIRECTIONAL SEARCH APPLICATION FOR POLAR CODES WITH LARGE KERNELS	161
<i>Ilya Morzharetto, Peter Trifonov</i>	
QUATERNARY REED – MULLER CODES AND THEIR MINIMUM WEIGHT BASES.....	166
<i>Faina I. Solov'Eva</i>	
EXTENDED EVENODD+ CODES WITH ASYMPTOTICALLY OPTIMAL UPDATES AND EFFICIENT ENCODING/DECODING	170
<i>Hong Fu, Hanxu Hou, Li Zhang</i>	
MULTI-SERVER PRIVATE LINEAR COMPUTATION WITH JOINT AND INDIVIDUAL PRIVACY GUARANTEES	176
<i>Nahid Esmati, Anoosheh Heidarzadeh, Alex Sprintson</i>	
MULTI-SERVER PRIVATE LINEAR TRANSFORMATION WITH JOINT PRIVACY	182
<i>Fatemeh Kazemi, Alex Sprintson</i>	
FIELD TRACE POLYNOMIAL CODES FOR SECURE DISTRIBUTED MATRIX MULTIPLICATION	188
<i>Roberto Assis Machado, Rafael G. L. D'Oliveira, Salim El Rouayheb, Daniel Heinlein</i>	

Author Index