

**2019 XVI International  
Symposium “Problems of  
Redundancy in Information and  
Control Systems”  
(REDUNDANCY 2019)**

**Moscow, Russia  
21 – 25 October 2019**



IEEE Catalog Number: CFP1971R-POD  
ISBN: 978-1-7281-1945-8

**Copyright © 2019 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:	CFP1971R-POD
ISBN (Print-On-Demand):	978-1-7281-1945-8
ISBN (Online):	978-1-7281-1944-1

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# Program

## 2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)

### LDPC and Polar codes

<i>Permutation Decoding of Polar Codes</i> Mikhail Kamenev (Huawei Technologies Co., Ltd., Russia), Yulia Kameneva (Huawei Technologies Co., Ltd., Russia), Oleg F Kurmaev (Huawei Technologies Co., Ltd., Russia), Alexey Maevskiy (Huawei Technologies Co., Ltd., Russia) .....	1
<i>Simplified Lower Bound on Minimum Distance of Convolutional Polar Codes</i> Ruslan Morozov (ITMO University, Russia) .....	7
<i>Design and Decoding of Polar Codes with a Mixture of Reed-Solomon and Arikian Kernels</i> Nikolai Iakuba (ITMO University, Russia), Peter Trifonov (Saint-Petersburg Polytechnic University & ITMO University, Russia) .....	12
<i>On the performance analysis of short LDPC codes</i> Luiza Medova (Moscow Institute of Physics and Mathematics & Institute for Information Transmission Problems (IITP RAS), Russia), Pavel Rybin (IITP RAS & Skoltech, HSE, Russia), Ivan Filatov (MIPT, Russia) .....	18
<i>On the Hard-Decision Multi-Threshold Decoding of Binary and Non-Binary LDPC Codes</i> Andrei I. Dzis (Moscow Institute of Physics and Technology & Skolkovo Institute of Science and Technology, Russia), Pavel Rybin (IITP RAS & Skoltech, HSE, Russia), Alexey A. Frolov (Skolkovo Institute of Science and Technology & IITP RAS, Russia) .....	23

### Coding for MAC and IoT

<i>On the Capacity Estimation of a Slotted Multiuser Communication Channel with Noise</i> Fedor Ivanov (National Research University Higher School of Economics & Institute for Information Transmission Problems, Russia), Alexey Kreshchuk (Institute for Information Transmission Problems, Russia), Pavel Rybin (IITP RAS & Skoltech, HSE, Russia), Valentin Afanassiev (Intitute Problems of Information Transmission, Russia) .....	27
<i>Error correcting coding schemes for a broadcast channels</i> Vladimir Potapov (Institute for Information Transmission Problems, Russia), Victor V. Zyablov (Institute for Information Transmission Problems (IITP) RAS, Russia) .....	32
<i>Coded Multitone Transmission in a DHA FH OFDMA system employing order statistics</i> Dmitry Osipov (IITP RAS, Russia) .....	36

### Combinatorics of codes

<i>On Minimal Distance between <math>q</math>-ary Plateaued Functions</i> Vladimir N Potapov (Sobolev Institute of Mathematics, Russia) .....	42
<i>A Lower Bound on the Number of Boolean Functions with Median Correlation Immunity</i> Vladimir N Potapov (Sobolev Institute of Mathematics, Russia) .....	45
<i>Reconstructing Sets of Latin Squares, Linear and Equivalent to Linear Codes</i> Evqeny V. Gorkunov (Sobolev Institute of Mathematics & Novosibirsk State University, Russia), Vitaly R. Danilko (Novosibirsk State University, Russia) .....	47
<i>New bounds for linear codes of covering radius 3 and 2-saturating sets in projective spaces</i> Alexander A. Davydov (Institute for Information Transmission Problems, Russian Academy of Sciences, Russia), Stefano Marcugini (Perugia University, Italy), Fernanda Pambianco (Perugia University, Italy) .....	52
<i>On two problems concerning universal bounds for codes</i> Peter Boyvalenkov (Institute of Mathematics and Informatics, Bulqarian Academy of Sciences & South-Western University, Blaqoevqrad, Bulqaria), Peter Draqnev (Purdue University Fort Wayne, USA), Douq Hardin (Vanderbilt University, USA), Edward Saff (Vadnerbilt University, USA), Maya Stoyanova (Sofia University, Bulgaria) .....	58

## Codes for storage

<i>Trivariate Lifted Codes with Disjoint Repair Groups</i> Nikita Polyanskiy (Skolkovo Institute of Science and Technology, Russia), Ilya Vorobyev (Skolkovo Institute of Science and Technology & Moscow Institute of Physics and Technology, Russia) .....	64
<i>Batch codes based on lifted multiplicity codes</i> Rina Polyanskaya (Institute for Information Transmission Problems, Russia), Nikita Polyanskiy (Skolkovo Institute of Science and Technology, Russia) .....	69
<i>Load Balancing Performance in Distributed Storage with Regular Balanced Redundancy</i> Mehmet Aktas (Rutgers University, USA), Amir Behrouzi-Far (Rutgers University, USA), Emina Soljanin (Rutgers University, USA) .....	75
<i>Unicast-Uniprior Index Coding Problems: Minrank and Criticality</i> Niranjana Ambadi (Indian Institute of Science, Bangalore, India) .....	81
<i>Error Correction for Partially Stuck Memory Cells</i> Haider Al Kim (Technical University of Munich (TUM), Germany & University of Kufa, Iraq), Sven Puchinger (Technical University of Munich, Germany), Antonia Wachter-Zeh (Technical University of Munich (TUM), Germany) .....	87

## Codes for different applications I

<i>New lower bound on the rate of traceability set systems</i> Elena Egorova (Skolkovo Institute of Science and Technology, Russia), Ilya Vorobyev (Skolkovo Institute of Science and Technology & Moscow Institute of Physics and Technology, Russia) .....	93
<i>Symmetric group testing with noise</i> Elena Egorova (Skolkovo Institute of Science and Technology, Russia) .....	99
<i>On Maximum-Likelihood Decoding of Time-Varying Trellis Codes</i> Wenhui Li (Skolkovo Institute of Science and Technology (Skoltech), Russia), Vladimir Sidorenko (Technical University of Munich, Germany), Thomas Jerkovits (German Aerospace Center (DLR), Germany), Gerhard Kramer (Technical University of Munich, Germany) .....	104
<i>The influence of active distances on the distribution of bursts</i> Anastasiia Smeshko (Institute for Information Transmission Problems & National Research University Higher School of Economics, Russia), Fedor Ivanov (National Research University Higher School of Economics & Institute for Information Transmission Problems, Russia), Victor V. Zyablov (Institute for Information Transmission Problems (IITP) RAS, Russia) .....	110

## Codes for different applications II

<i>Construction of the solution of the Chinese Remainder Theorem for polynomials using the method of undetermined coefficients</i> Serqei V. Fedorenko (National Research University Higher School of Economics, Russia), Andrey Krouk (State University of Aerospace Instrumentation & National Research University Higher School of Economics, Russia) .....	115
<i>New class of codes, correcting errors in the Lee metric</i> Viacheslav Davydov (National Research University Higher School of Economics, Russia) .....	117
<i>Efficient Decoding of Interleaved Low-Rank Parity-Check Codes</i> Julian Renner (Technical University of Munich, Germany), Thomas Jerkovits (German Aerospace Center (DLR), Germany), Hannes Bartz (German Aerospace Center, Germany) .....	121

## Cryptography and codes

<i>Interleaving Loidreau's Rank-Metric Cryptosystem</i> Julian Renner (Technical University of Munich, Germany), Sven Puchinger (Technical University of Munich, Germany), Antonia Wachter-Zeh (Technical University of Munich (TUM), Germany) .....	127
<i>On the Lightweight McEliece Cryptosystem for Low-Power Devices</i> Fedor Ivanov (National Research University Higher School of Economics & Institute for Information Transmission Problems, Russia), Evqenii Krouk (Higher School of Economics, Russia), Alexey Kreshchuk (Institute for Information Transmission Problems, Russia) .....	133

<i>Parallel algorithms for solving sparse binary subset sums using random mappings</i> Nikita Rumenco (Moscow Institute of Physics and Technology, Russia), Alexander V Kostyuck (Moscow Institute of Physics and Technology, Russia) .....	139
<i>On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes</i> Yury Kosolapov (Southern Federal University, Russia), Vladimir Deundyak (Southern Federal University, Russia) .....	143
<i>Channel Models for Physical Unclonable Functions based on DRAM Retention Measurements</i> Sven Müelich (Ulm University, Germany), Sebastian Bitzer (Ulm University, Germany), Chirag Sudarshan (Technical University of Kaiserslautern, Germany), Christian Weis (University of Kaiserslautern, Germany), Norbert Wehn (University of Kaiserslautern, Germany), Martin Bossert (Ulm University, Germany), Robert F.H. Fischer (Ulm University, Germany) .....	149
<i>Challenges beyond blockchain: scaling, oracles and privacy preserving</i> Stanislav Krualik (Skolkovo Institute of Science and Technology, Russia), Kamilla Nazirkhanova (Moscow Institute of Physics and Technology & Institute for Information Transmission Problems RAS, Russia), Yury Yanovich (Institute for Information Transmission Problems, Russia) .....	155

## Machine learning

<i>Research of heuristic approaches for determining the tonality of text messages in natural language processing problems</i> Evgeniy Polyakov (National Research University Higher School of Economics, Russia), Serqey Polyakov (Moscow Aviation Institute National Research University, Russia), Pavel Sergeevich Abramov (Higher School of Economics, Russia) .....	159
<i>End-to-end Deep Object Tracking with Circular Loss Function for Rotated Bounding Box</i> Vladislav Belayev (JetBrains Research & St Peterburg Higher School of Economics, Russia), Aleksandra Malysheva (Higher School of Economics, Russia), Aleksei Shpilman (JetBrains Research & National Research University Higher School of Economics, Russia) .....	165
<i>Multi-agent Graph Network for Deep Multi-agent Reinforcement Learning</i> Aleksandra Malysheva (Higher School of Economics, Russia), Daniel Kudenko (L3S Research Center Leibniz University Hannover, Germany), Aleksei Shpilman (JetBrains Research & National Research University Higher School of Economics, Russia) .....	171
<i>Methodology of Mean Shift Clustering Algorithm Implementation Based on Dataflow Computer</i> Serqey Mikhailovich Salibekyan (National Research University Higher School of Economics, Russia), Elena M. Ivanova (National Research University Higher School of Economics, Russia), Andrey Vishnekov (Higher School of Economics, Russia) .....	177
<i>Curve Fitting for Error Rate Data</i> Alexander B. Sergienko (St.-Petersburg Electrotechnical University, Russia) .....	181

## Different aspects of IoT

<i>Computer Capacity As a Tool For the Processors Development Analysis</i> Anton Rakitskiy (Siberian State University of Telecommunications and Information Science & Novosibirsk State University, Russia), Boris Ryabko (Institute of Computational Technologies of SB RAS & Novosibirsk State University, Russia) .....	186
<i>DC Designer: Software System of Scaling Multiprovider Data Centers Networks</i> Dmitry Perepelkin (RSREU, Russia), Maria Ivanchikova (Ryazan State Radio Engineering University, Russia) .....	191
<i>SDN Cluster Constructor: Software Toolkit for Structures Segmentation of Software Defined Networks</i> Dmitry Perepelkin (RSREU, Russia), Ilya Tsyganov (Ryazan State Radio Engineering University, Russia) .....	195
<i>Data Delivery Efficient Spreading Factor Allocation in Dense LoRaWAN Deployments</i> Oleg Gusev (IOT Laboratory Ltd., Russia), Andrey Turlikov (Saint-Petersburg State University of Aerospace Instrumentation, Russia), Semen Andreevich Kuzmichev (Saint Petersburg State University of Aerospace Instrumentation, Russia), Nikita Stepanov (Saint Petersburg State University of Aerospace Instrumentation, Russia) .....	199
<i>Study of the energy consumption of graphical interfaces on TFT displays</i> Alexey Rolich (National Research University Higher School of Economics, Russia), Sofia Saprykina (National Research University Higher School of Economics, Russia), Elizaveta Fedotova (National Research University Higher School of Economics, Russia) .....	205

# Data security and related topics

## *Gradient Cryptanalysis of Block Cipher CHAM 64/128*

Adrey Fionov (Siberian State University of Telecommunications, Russia), Boris Ryabko (Institute of Computational Technologies of SB RAS & Novosibirsk State University, Russia), Alexander Soskov (Institute of Computational Technologies SB RAS, Russia) ..... 211

## *Application of list decoding of convolutional codes to steganography*

Klim Kireev (Skolkovo Institute of Science and Technology, Russia), Griqorii Melnikov (Skolkovo Institute of Science and Technology, Russia), Edqar Kaziakhmedov (Skolkovo Institute of Physics and Technology & Moscow Institute of Physics and Technology, Russia) ..... 216

## *Transparent E-voting dApp Based on Waves Blockchain and RIDE Language*

Nazim Faour (National Research University-Higher School of Economics & Waves Platform, Russia) ..... 219

## *Achievability Bounds for Massive Random Access in the Gaussian MAC with Delay Constraints*

Artem Burkov (State University of Aerospace Instrumentation Saint-Petersburg, Russia), Alexey A. Frolov (Skolkovo Institute of Science and Technology & IITP RAS, Russia), Pavel Rybin (IITP RAS & Skoltech, HSE, Russia), Andrey Turlikov (Saint-Petersburg State University of Aerospace Instrumentation, Russia) ..... 224