

2014 IEEE Information Theory Workshop

(ITW 2014)

**Hobart, Australia
2-5 November 2014**



**IEEE Catalog Number: CFP14ITW-POD
ISBN: 978-1-4799-6000-2**

TABLE OF CONTENTS

Mo1A : Algebraic Network Information Theory

How to Design an Efficient Lattice Coding Scheme	1
---	----------

Ram Zamir (Tel Aviv University, Israel)

Compute-and-Forward for Discrete Memoryless Networks	5
---	----------

Bobak Nazer (Boston University, USA) and Michael Gastpar (EPFL & University of California, Berkeley, Switzerland)

Lattices from Codes for Harnessing Interference : An Overview and Generalizations	10
--	-----------

Yu-Chih Huang (Texas A&M University, USA) and Krishna Narayanan (Texas A&M University, USA)

Generalized Low-Density (GLD) Lattices	15
---	-----------

Joseph Jean Boutros (Texas A&M University at Qatar, Qatar), Nicola di Pietro (Texas A&M University at Qatar, Qatar) and Nour Basha (Texas A&M University at Qatar, Qatar)

Message Variance Convergence Condition for Generalizations of LDLC Lattices	20
--	-----------

Brian Michael Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan) and Ricardo Antonio Parrao Hernandez (Japan Advanced Institute of Science and Technology, Japan)

Mo1B : Physical Layer Security

The Multiple Access Channel with an Untrusted Relay	25
--	-----------

Ahmed A Zewail (The Pennsylvania State University, USA) and Aylin Yener (Pennsylvania State University, USA)

Reliable Deniable Communication with Channel Uncertainty	30
---	-----------

Pak Hou Che (The Chinese University of Hong Kong, Hong Kong), Mayank Bakshi (The Chinese University of Hong Kong, Hong Kong), Chung Chan (The Chinese University of Hong Kong, Hong Kong) and Sidharth Jaggi (Chinese University of Hong Kong, Hong Kong)

A New Upperbound for the Oblivious Transfer Capacity of Discrete Memoryless Channels	35
---	-----------

Sankeerth Rao (IIT Bombay, India) and Vinod M Prabhakaran (Tata Institute of Fundamental Research, India)

An Efficient Code for Adversarial Wiretap Channel	40
--	-----------

Pengwei Wang (University of Calgary, Canada) and Reihaneh Safavi-Naini (University of Calgary, Canada)

Interactive Code to Correct and Detect Omniscient Byzantine Adversaries	45
--	-----------

Zhiqing Xiao (Tsinghua University, P.R. China), Yunzhou Li (Tsinghua University, P.R. China), Ming Zhao (Tsinghua University, P.R. China) and Jing Wang (EE. Tsinghua University, P.R. China)

Mo1C : Codes for Storage I

Linear Programming Bounds for Robust Locally Repairable Storage Codes	50
--	-----------

Ali Tebbi (University of South Australia, Australia), Terence H. Chan (University of South Australia, Australia) and Chi Wan Sung (City University of Hong Kong, Hong Kong)

A Code Design Framework for Multi-Rack Distributed Storage 55

Ali Tebbi (University of South Australia, Australia), Terence H. Chan (University of South Australia, Australia) and Chi Wan Sung (City University of Hong Kong, Hong Kong)

Locally Repairable RapidRAID Systematic Codes – One simple convoluted way to get it all 60

Anwitaman Datta (Nanyang Technological University, Singapore)

The Fundamental Theorem of Distributed Storage Systems Revisited 65

Ping Hu (City University of Hong Kong, Hong Kong), Kenneth W. Shum (Institute of Network Coding, Hong Kong) and Chi Wan Sung (City University of Hong Kong, Hong Kong)

Locally Repairable Codes over a Network 70

Quan Yu (City University of Hong Kong, Hong Kong), Chi Wan Sung (City University of Hong Kong, Hong Kong) and Terence H. Chan (University of South Australia, Australia)

Mo2A : Reductive Arguments for Network Information Theory

Reductions Techniques for Establishing Equivalence Between Different Classes of Network and Index Coding Problems 75

Alex Sprintson (Texas A&M University, USA)

A Few Meta-Theorems in Network Information Theory 77

Yu Xiang (University of California, San Diego, USA) and Young-Han Kim (UCSD, USA)

Is there a canonical network for network information theory? 82

Michelle Effros (California Institute of Technology, USA) and Michael Langberg (State University of New York at Buffalo, USA)

Mo2B : Interference Alignment

Cyclic Interference Alignment and Cancellation in 3-User X-Networks with Minimal Backhaul . . 87

Henning Maier (RWTH Aachen University, Germany) and Rudolf Mathar (RWTH Aachen University, Germany)

Symmetric Degrees of Freedom of the MIMO 3-Way Channel with $M_T \times M_R$ Antennas 92

Henning Maier (RWTH Aachen University, Germany), Anas Chaaban (Ruhr-Universität Bochum, Germany) and Rudolf Mathar (RWTH Aachen University, Germany)

On Achievable Degrees of Freedom of 3-user MIMO Interference Channels 97

Lu Yang (University of New South Wales, Australia) and Wei Zhang (The University of New South Wales, Australia)

On Feasibility of Linear Interference Alignment with Symbol Extension for Two-Cell MIMO Interfering Multiple Access Channel 102

Edin Zhang (Yuan Ze University, Taiwan) and Chiachi Huang (Yuan Ze University, Taiwan)

Enabling the Multi-User Generalized Degrees of Freedom in the Gaussian Cellular Channel . . . 107

Rick Fritschek (Berlin Institute of Technology, Germany) and Gerhard Wunder (Heinrich-Hertz-Institut, Germany)

Mo2C : Lattice Codes

The Semantic Secrecy Rate of the Lattice Gaussian Coding for the Gaussian Wiretap Channel . 112

Hamed Mirghasemi (Telecom ParisTech, France) and Jean-Claude Belfiore (Ecole Nationale Supérieure des Télécommunications, France)

Construction and Secrecy Gain of a Family of 5-modular Lattices 117

Xiaolu Hou (Nanyang Technological University, Singapore), Fuchun Lin (Imperial College London, Singapore) and Frederique Oggier (Nanyang Technological University, Singapore)

Arithmetic Geometry of Compute and Forward 122

Angeles Vazquez-Castro (Universidad Autónoma de Barcelona, Spain)

Shaping Low-Density Lattice Codes Using Voronoi Integers 127

Nuwan S. Ferdinand (University of Oulu, Finland), Brian Michael Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan), Behnaam Aazhang (Rice University, USA) and Matti Latva-aho (UoOulu, Finland)

On the Ice-Wine Problem : Recovering Linear Combination of Codewords over the Gaussian Multiple Access Channel 132

Shahab Ghasemi-Goojani (Sharif University of Technology, Iran) and Hamid Behrooz (Sharif University of Technology, Iran)

Mo3A : Classical Coding Theory

Relative Generalized Hamming Weights of One-Point Algebraic Geometric Codes 137

Olav Geil (Aalborg University, Denmark), Stefano Martin (Aalborg University, Denmark), Ryutaroh Matsumoto (Tokyo Institute of Technology, Japan), Diego Ruano (Aalborg University, Denmark) and Yuan Luo (Shanghai Jiao Tong University, P.R. China)

Rank weight hierarchy of some classes of cyclic codes 142

Jerome Ducoat (Nanyang Technological University, Singapore) and Frederique Oggier (Nanyang Technological University, Singapore)

Gilbert-Varshamov-like Lower Bounds for Deletion-Correcting Codes 147

Frederic Sala (University of California, Los Angeles, USA), Ryan Gabrys (UCLA, USA) and Lara Dolecek (UCLA, USA)

Repeated Deletion Channels 152

Bernhard Haeupler (Microsoft Research, USA) and Michael Mitzenmacher (Harvard University, USA)

A Complete MacWilliams Theorem for Convolutional Codes	157
<i>Ching-Yi Lai (University of Technology, Sydney, Australia), Min-Hsiu Hsieh (University of Technology, Sydney, Australia) and Hsiao-feng Francis Lu (National Chiao Tung University, Taiwan)</i>	

Syndrome Decoding of Symbol-Pair Codes	162
<i>Masanori Hirotomo (Saga University, Japan), Makoto Takita (Kobe University, Japan) and Masakatu Morii (Kobe University, Japan)</i>	

Mo3B : Coding and Inf. Theory Applications

Feedback Systems using Non-Binary LDPC Codes with a Limited Number of Transmissions . . .	167
<i>Kasra Vakilinia (University of California, Los Angeles (UCLA), USA), Adam Williamson (University of California, Los Angeles, USA), Sudarsan Vasista Srinivasan Ranganathan (University of California, Los Angeles, USA), Dariush Divsalar (Jet Propulsion Laboratory, USA) and Richard Wesel (University of California, Los Angeles, USA)</i>	

Quantum Synchronizable Codes From Quadratic Residue Codes and Their Supercodes	172
<i>Yixuan Xie (University of New South Wales, Australia), Jinhong Yuan (University of New South Wales, Australia) and Yuichiro Fujiwara (California Institute of Technology, USA)</i>	

On the Capacity and the Zero-Error Capacity of k-Resilient AND Anti-Collusion Codes	177
<i>Hiroki Koga (University of Tsukuba, Japan)</i>	

Haplotype Assembly : An Information Theoretic View	182
<i>Hongbo Si (The University of Texas at Austin, USA), Haris Vikalo (The University of Texas at Austin, USA) and Sriram Vishwanath (University of Texas Austin, USA)</i>	

Spatially-Coupled Counter Braids	187
<i>Eirik Rosnes (University of Bergen, Norway)</i>	

S-AMP : Approximate Message Passing for General Matrix Ensembles	192
<i>Burak Çakmak (Aalborg University, Denmark), Ole Winther (Technical University of Denmark, Denmark) and Bernard Henri Fleury (Aalborg University, Denmark)</i>	

Mo3C : Source Coding

Variable-length Lossy Source Code Using a Constrained-Random-Number Generator	197
<i>Jun Muramatsu (NTT Corporation, Japan)</i>	

Revisiting the Rate-Distortion Theory Using Smooth Max Renyi Divergence	202
<i>Tomohiko Uyematsu (Tokyo Institute of Technology, Japan) and Tetsunao Matsuta (Tokyo Institute of Technology, Japan)</i>	

Delay Exponent of Variable-Length Random Binning for Point-to-Point Transmission	207
<i>Badri N Vellambi (University of South Australia, Australia), Nan Zhang (University of South Australia, Australia)</i>	

and Khoa D. Nguyen (University of South Australia, Australia)

Fundamental Limits of Universal Lossless One-to-One Compression of Parametric Sources 212

Ahmad Beirami (Duke University, USA) and Faramarz Fekri (Georgia Institute of Technology, USA)

Using T-Codes as Locally Decodable Source Codes 217

Ulrich Speidel (University of Auckland, New Zealand), T. Aaron Gulliver (University of Victoria, Canada), Ali Makhdoumi (MIT, USA) and Muriel Médard (MIT, USA)

Stochastic Complexity for Tree Models 222

Junichi Takeuchi (Kyushu University, Japan) and Andrew R Barron (Yale University, USA)

Tu1A : Physical Layer security and privacy in cyber and cyber physical systems

Reliable, Deniable and Hidable Communication : A quick survey 227

Pak Hou Che (The Chinese University of Hong Kong, Hong Kong), Swanand Kadhe (Texas A&M University, USA), Mayank Bakshi (The Chinese University of Hong Kong, Hong Kong), Chung Chan (The Chinese University of Hong Kong, Hong Kong), Sidharth Jaggi (Chinese University of Hong Kong, Hong Kong) and Alex Sprintson (Texas A&M University, USA)

Coding for Wiretap Channels : Channel Resolvability and Semantic Security 232

Andrew Thangaraj (IIT Madras, India)

On the Oblivious Transfer Capacity Region of the Binary Erasure Broadcast Channel 237

Manoj Mishra (Indian Institute of Technology - Bombay, India), Bikash K Dey (Indian Institute of Technology Bombay, India), Vinod M Prabhakaran (Tata Institute of Fundamental Research, India) and Suhas Diggavi (University of California Los Angeles, USA)

Under the Radar Attacks in Dynamical Systems : Adversarial Privacy Utility Tradeoffs 242

Parth Pradhan (Lehigh University, USA) and Parv Venkitasubramaniam (Lehigh University, USA)

On Generalized Active Attacks by Causal Adversaries in Networks 247

Oliver Kosut (Arizona State University, USA) and Li-Wei Kao (Arizona State University, USA)

Tu1B : Shannon Theory

An Exploration of the Role of Principal Inertia Components in Information Theory 252

Flavio P. Calmon (Massachusetts Institute of Technology, USA), Mayank Varia (Massachusetts Institute of Technology, Lincoln Laboratory, USA) and Muriel Médard (MIT, USA)

Rényi Entropy and Quantization for Densities 257

Christoph Bunte (ETH Zurich, Switzerland) and Amos Lapidoth (ETHZ, Switzerland)

Capacity Bounds for certain Channels with States and the Energy Harvesting Channel 262

Wei Mao (California Institute of Technology, USA) and Babak Hassibi (California Institute of Technology, USA)

Searching with Measurement Dependent Noise	267
<i>Yonatan Kaspı (UCSD, USA), Ofer Shayevitz (Tel Aviv University, Israel) and Tara Javidi (UCSD, USA)</i>	

Correlation between Channel State and Information Source with Empirical Coordination Constraint	272
<i>Mael Le Treust (ETIS, CNRS, ENSEA, University Cergy-Pontoise, France)</i>	

Tu1C : MIMO

Unitary Precoding for Integer-Forcing MIMO Linear Receivers	277
<i>Amin Sakzad (Monash University, Australia) and Emanuele Viterbo (Monash University, Australia)</i>	

Performance of Precoded Integer-Forcing for Closed-Loop MIMO Multicast	282
<i>Elad Domanovitz (Tel Aviv University, Israel) and Uri Erez (Tel Aviv University, Israel)</i>	

Multi-Dimensional and Non-Uniform Constellation Optimization via the Special Orthogonal Group	287
<i>David Karpuk (Aalto University, Finland) and Camilla Hollanti (Aalto University, Finland)</i>	

Effects of Mobility on User Energy Consumption and Total Throughput in a Massive MIMO System	292
<i>Aris Moustakas (University of Athens, Greece), Luca Sanguinetti (University of Pisa, Italy) and M��rouane Debbah (Supelec, France)</i>	

Multicell Coordinated Scheduling with Multiuser ZF Beamforming : Policies and Performance Bounds	297
<i>Min Li (Macquarie University, Australia), Iain B. Collings (CSIRO, Australia), Stephen Hanly (Macquarie University, Australia), Chunshan Liu (Macquarie University, Australia) and Philip Whiting (Macquarie University, Australia)</i>	

Sparse Bayesian Learning Approach for Streaming Signal Recovery	302
<i>Uditha L. Wijewardhana (University of Oulu & Centre for Wireless Communications, Finland) and Marian Codreanu (University of Oulu, Finland)</i>	

Tu2A : Coding for wiretap channels

Codes for Wireless Wiretap Channels	307
<i>Jean-Claude Belfiore (Ecole Nationale Sup��rieure des T��l��communications, France)</i>	

On Measures of Information Theoretic Security	309
<i>Shuiyin Liu (Monash University, Australia), Yi Hong (Monash University, Australia) and Emanuele Viterbo (Monash University, Australia)</i>	

Superposition Lattice Coding for Gaussian Broadcast Channel with Confidential Message	311
<i>Li Chia Choo (Institute for Infocomm Research, Singapore) and Cong Ling (Imperial College London, United Kingdom)</i>	

A USRP Implementation of Wiretap Lattice Codes	316
---	------------

Jinlong Lu (Nanyang Technological University, Singapore), J Harshan (Nanyang Technological University, Singapore) and Frederique Oggier (Nanyang Technological University, Singapore)

Key Capacity Region for a Cellular Source Model 321

Huishuai Zhang (Syracuse University, USA), Yingbin Liang (Syracuse University, USA) and Lifeng Lai (Worcester Polytechnic Institute, USA)

Tu2B : Fundamental Limits of Communications with Energy Harvesting

Max-min Fair Wireless Energy Transfer for Secure Multiuser Communication Systems 326

Derrick Wing Kwan Ng (Friedrich-Alexander-University Erlangen-Nürnberg, Germany) and Robert Schober (University of British Columbia, Canada)

Capacity of the Energy Harvesting Channel with Energy Arrival Information at the Receiver . . . 331

Omur Ozel (University of Maryland, College Park, USA), Kaya Tutuncuoglu (Pennsylvania State University, USA), Sennur Ulukus (University of Maryland, USA) and Aylin Yener (Pennsylvania State University, USA)

State Amplification and State Masking for the Binary Energy Harvesting Channel 336

Kaya Tutuncuoglu (Pennsylvania State University, USA), Omur Ozel (University of Maryland, College Park, USA), Aylin Yener (Pennsylvania State University, USA) and Sennur Ulukus (University of Maryland, USA)

Recent Advances in Joint Wireless Energy and Information Transfer 341

*Suzhi Bi (National University of Singapore, Singapore), Chin Keong Ho (Institute for Infocomm Research, A*STAR, Singapore) and Rui Zhang (National University of Singapore, Singapore)*

Tu2C : Emerging Applications of Information Theory

Inferring the dynamic range of electrode current by using an information theoretic model of cochlear implant stimulation 346

Xiao Gao (Institute for Telecommunications Research, University of South Australia, Australia), David B Grayden (University of Melbourne, Australia) and Mark D McDonnell (University of South Australia, Australia)

On ℓ_p -norm Computation over Multiple-Access Channels 351

Steffen Limmer (Fraunhofer Heinrich Hertz Institute, Germany) and Slawomir Stanczak (Fraunhofer Heinrich Hertz Institute & Technische Universität Berlin, Germany)

Can we measure the difficulty of an optimization problem? 356

Tansu Alpcan (The University of Melbourne, Australia), Tom Everitt (Stockholm University, Sweden) and Marcus Hutter (Australian National University, Australia)

Secure Degrees of Freedom Region of the Gaussian Interference Channel with Secrecy Constraints 361

Jianwei Xie (Google Inc., USA) and Sennur Ulukus (University of Maryland, USA)

Tu3A : Polar Codes

Polarization as a novel architecture to boost the classical mismatched capacity of B-DMCs . . .	366
<i>Mine Alsan (EPFL, Switzerland) and Emre Telatar (EPFL, Switzerland)</i>	
Universal Polar Decoding with Channel Knowledge at the Encoder	371
<i>Mine Alsan (EPFL, Switzerland)</i>	
Sequential Decoding of Polar Codes with Arbitrary Binary Kernel	376
<i>Vera Miloslavskaya (Saint-Petersburg State Polytechnical University, Russia) and Peter Trifonov (Saint-Petersburg State Polytechnic University, Russia)</i>	
A New Multiple Folded Successive Cancellation Decoder for Polar Codes	381
<i>Harish Vangala (Monash University & Indian Institute of Science, Australia), Emanuele Viterbo (Monash University, Australia) and Yi Hong (Monash University, Australia)</i>	
Successive Cancellation Permutation Decoding of Reed-Solomon Codes	386
<i>Peter Trifonov (Saint-Petersburg State Polytechnic University, Russia)</i>	

Tu3B : Network Coding I

Decoding Delay Reduction in Network Coded Cooperative Systems with Intermittent Status Update	391
<i>Mohammad S. Karim (The Australian National University, Australia), Neda Aboutorab (The Australian National University, Australia), Ali A Nasir (Australian National University, Australia) and Parastoo Sadeghi (The Australian National University, Australia)</i>	
Locality-Preserving Secure Network Coding	396
<i>Xuan Guang (Nankai University, P.R. China), Jiyong Lu (Nankai University, P.R. China) and Fang-Wei Fu (Nankai University, P.R. China)</i>	
Inter-session Network Coding for Transmitting Multiple Layered Streams over Single-hop Wireless Networks	401
<i>Mohammad Esmaeilzadeh (Australian National University, Australia) and Neda Aboutorab (The Australian National University, Australia)</i>	
From LDPC to Chunked Network Codes	406
<i>Shenghao Yang (Tsinghua University, P.R. China) and Bin Tang (Nanjing University, P.R. China)</i>	

Tu3C : Secure Broadcast Channel

Feedback Enhances the Security of Degraded Broadcast Channels with Confidential Messages and Causal Channel State Information	411
<i>Bin Dai (Southwest Jiaotong University, P.R. China) and Zheng Ma (Southwest Jiaotong University, P.R. China)</i>	
Secure Communication of Correlated Sources over Broadcast Channels	416
<i>Fei Lang (Nanjing University of Posts and Telecommunications, P.R. China), Zhixiang Deng (Hohai University, P.R. China) and Bao-Yun Wang (Nanjing University of Posts & Telecommunications, P.R. China)</i>	

On the Secrecy Capacity Region of the Wiretap Broadcast Channel	421
<i>Meryem Benammar (SUPELEC, France) and Pablo Piantanida (SUPELEC, France)</i>	

Secrecy Measures for Broadcast Channels With Receiver Side Information : Joint vs Individual .	426
<i>Ahmed Mansour (Technische Universität München, Germany), Rafael F. Schaefer (Princeton University, USA) and Holger Boche (Technical University Munich, Germany)</i>	

Capacity estimation of two-dimensional channels using Sequential Monte Carlo	431
<i>Christian A. Naesseth (Linköping University, Sweden), Fredrik Lindsten (Linköping University, Sweden) and Thomas B. Schön (Uppsala University, Sweden)</i>	

We1A : Graph-based Codes

Explicit Constructions for Type-1 QC-LDPC Codes with Girth at Least Ten	436
<i>Juhua Wang (China Academy of Space Technology (Xi'an), P.R. China), Guohua Zhang (China Academy of Space Technology (Xi'an), P.R. China), Quan Zhou (China Academy of Space Technology (Xi'an), P.R. China), Yang Yang (Chang'an University, P.R. China) and Rong Sun (Xidian University, P.R. China)</i>	

LT Code Design for Inactivation Decoding	441
<i>Francisco Lázaro Blasco (German Aerospace Center (DLR), Germany), Gianluigi Liva (DLR - German Aerospace Center, Germany) and Gerhard Bauch (Hamburg University of Technology, Germany)</i>	

Non-Uniform Spatial Coupling	446
<i>Fanny Jardel (Télécom ParisTech, France) and Joseph Jean Boutros (Texas A&M University at Qatar, Qatar)</i>	

Delay-Exponent of Bilayer Anytime Code	451
<i>Md Noor-A-Rahim (University of South Australia, Australia), Khoa D. Nguyen (University of South Australia, Australia) and Gottfried Lechner (University of South Australia, Australia)</i>	

Optimization of Graph Based Codes for Belief Propagation Decoding	456
<i>Sachini Jayasooriya (University of Newcastle, Australia), Sarah J Johnson (University of Newcastle, Australia), Lawrence Ong (The University of Newcastle, Australia) and Regina Berretta (The University of Newcastle, Australia)</i>	

Design of Non-Binary Quasi-Cyclic LDPC Codes by Absorbing Set Removal	461
<i>Behzad Amiri (UCLA, USA), Jorge Arturo Flores Castro (Instituto Nacional de Astrofísica Óptica y Electrónica (INAOE), Mexico) and Lara Dolecek (UCLA, USA)</i>	

We1B : Multiple Access Channel

Low-Complexity Channel Resolvability Codes for the Symmetric Multiple-Access Channel . . .	466
<i>Remi A Chou (Georgia Institute of Technology, USA), Matthieu Bloch (Georgia Institute of Technology & Georgia Tech Lorraine, France) and Joerg Kliewer (New Jersey Institute of Technology, USA)</i>	

Enhanced Trellis Coded Multiple Access (ETCMA)	471
---	------------

Alberto G. Perotti (Huawei Technologies Sweden AB, Sweden) and Branislav M. Popovic (Huawei Technologies Sweden AB, Sweden)

Posterior Matching Scheme for Gaussian Multiple Access Channel with Feedback 476

Lan V. Truong (FPT University, Vietnam)

Linearly-Coupled Fountain Codes for Network-Coded Multiple Access 481

Shenghao Yang (Tsinghua University, P.R. China), Soung Chang Liew (The Chinese University of Hong Kong, Hong Kong), Lizhao You (The Chinese University of Hong Kong, Hong Kong) and Yi Chen (The City University of Hong Kong, Hong Kong)

On the Adaptive Capacity Region of Fading MACs with Distributed CSI 486

Sreejith Sreekumar (IIT Bombay, India), Sibi Raj B Pillai (IIT Bombay, India) and Bikash K Dey (Indian Institute of Technology Bombay, India)

The Capacity of the Multiple Access Channel Under Distributed Scheduling and MMSE Decoding 491

Joseph Kampeas (Ben-Gurion University of the Negev, Israel), Asaf Cohen (Ben-Gurion University of the Negev, Israel) and Omer Gurewitz (Ben Gurion University, Israel)

We1C : Cryptography

How to Securely Compute the Modulo-Two Sum of Binary Sources 496

Deepesh Data (Tata Institute of Fundamental Research, Mumbai, India), Bikash K Dey (Indian Institute of Technology Bombay, India), Manoj Mishra (Indian Institute of Technology - Bombay, India) and Vinod M Prabhakaran (Tata Institute of Fundamental Research, India)

From the Information Bottleneck to the Privacy Funnel 501

Ali Makhdoumi (MIT, USA), Salman Salamatian (EPFL, Switzerland), Nadia Fawaz (Technicolor, USA) and Muriel Médard (MIT, USA)

Distributed Storage for Data Security 506

Annina Bracher (ETH Zurich, Switzerland), Amos Lapidoth (ETHZ, Switzerland) and Eran Hof (Samsung Israel Research and Development Center (SIRC), Israel)

A New Model of Client-Server Communications under Information Theoretic Security 511

Mitsugu Iwamoto (The University of Electro-Communications, Japan), Tsukasa Omino (Toshiba Corporation, Japan), Yuichi Komano (Toshiba Corporation, Japan) and Kazuo Ohta (University of Electro-Communications, Japan)

Efficient Secret Sharing Schemes Achieving Optimal Information Rate 516

Yongge Wang (University of North Carolina at Charlotte, USA) and Yvo Desmedt (UCL, United Kingdom)

An Elementary Completeness Proof for Secure Two-Party Computation Primitives 521

Ye Wang (Mitsubishi Electric Research Laboratories, USA), Prakash Ishwar (Boston University, USA) and Shantanu Rane (Palo Alto Research Center, USA)

We2A : Network Coding II

A Recursive Coding Algorithm for Two-unicast-Z Networks 526

Weifei Zeng (MIT, USA), Viveck Cadambe (MIT, USA) and Muriel Médard (MIT, USA)

A Matrix Completion Approach to Linear Index Coding Problem 531

Homa Esfahanizadeh (University of Tehran, Iran), Farshad Lahouti (Caltech Institute of Technology, USA) and Babak Hassibi (California Institute of Technology, USA)

On Deterministic Linear Network Coded Broadcast and Its Relation to Matroid Theory 536

Mingchao Yu (The Australian National University, Australia), Parastoo Sadeghi (The Australian National University, Australia) and Neda Aboutorab (The Australian National University, Australia)

On Index Coding and Graph Homomorphism 541

Javad B. Ebrahimi (The Chinese University of Hong Kong & Institute of Network Coding (INC), Hong Kong) and Mahdi Jafari Siavoshani (Sharif University of Technology, Iran)

On the Solvability of Three-Pair Networks With Common Bottleneck Links 546

Kai Cai (University of Hong Kong, Hong Kong) and Guangyue Han (University of Hong Kong, Hong Kong)

We2B : Broadcast Channel

Dirty Interference Cancellation for Gaussian Broadcast Channels 551

Ruchen Duan (Syracuse University, USA), Yingbin Liang (Syracuse University, USA), Ashish Khisti (University of Toronto, Canada) and Shlomo (Shitz) Shamai (The Technion, Israel)

Distributed Decode-Forward for Broadcast 556

Sung Hoon Lim (EPFL, Switzerland), Kwang Taik Kim (Samsung Electronics, Korea) and Young-Han Kim (UCSD, USA)

On Capacity of the Dirty Paper Channel with Fading Dirt in the Strong Fading Regime 561

Stefano Rini (National Chiao Tung University, USA) and Shlomo (Shitz) Shamai (The Technion, Israel)

Multiple Description Coding for the Compound Broadcast Channel 566

Meryem Benammar (SUPELEC, France), Pablo Piantanida (SUPELEC, France) and Shlomo (Shitz) Shamai (The Technion, Israel)

Coding Schemes for a Class of Receiver Message Side Information in AWGN Broadcast Channels 571

Behzad Asadi (The University of Newcastle, Australia), Lawrence Ong (The University of Newcastle, Australia) and Sarah J Johnson (University of Newcastle, Australia)

We2C : Coding Techniques

Concatenated Permutation Block Codes for Correcting Single Transposition Errors 576

Reolyn Heymann (University of Johannesburg, South Africa), Jos H. Weber (Delft University of Technology, The

Netherlands), Theo G. Swart (University of Johannesburg, South Africa) and Hendrik C Ferreira (University of Johannesburg, South Africa)

Iterative List-Decoding of Gabidulin Codes via Gröbner Based Interpolation 581

Margreta Kuijper (University of Melbourne, Australia) and Anna-Lena Trautmann (University of Melbourne & Monash University, Australia)

Achieving Positive Rates over AWGN Channels with Quantized Feedback and Linear Processing 586

Stefan Farthofer (Vienna University of Technology, Austria), Andreas Winkelbauer (Vienna University of Technology, Austria) and Gerald Matz (Vienna University of Technology, Austria)

A New Construction of Zero Correlation Zone Sequences from Generalized Reed-Muller Codes . 591

Zilong Liu (Nanyang Technological University, Singapore), Yong Liang Guan (Nanyang Technological University, Singapore) and Udaya Parampalli (The University of Melbourne, Australia)

Insertion and Deletion Errors with a Forbidden Symbol 596

Ankur A. Kulkarni (Indian Institute of Technology Bombay, India)

We3A : Codes for Storage II Construction of Random Input-Output Codes with Moderate Block Lengths 601

Ravi Hiranand Motwani (Intel Corporation, USA) and Eitan Yaakobi (Technion, Israel)

Local Rank Modulation for Flash Memories 606

Tuvi Etzion (Technion-Israel Institute of Technology, Israel) and Michal Horovitz (Technion - Israel Institute of Technology, Israel)

Quasi-Primitive Block-wise Concatenated BCH Codes for NAND Flash Memories 611

Daesung Kim (KAIST, Korea) and Jeongseok Ha (KAIST, Korea)

Set Avoidance Probabilities and Bounds on the Reliability of Erasure Coded Storage Systems . . 616

Antonio Campello (University of Campinas, Brazil) and Vinay A. Vaishampayan (DIMACS, Rutgers University & Columbia University, USA)

Almost Affine Locally Repairable Codes and Matroid Theory 621

Thomas Westerbäck (Aalto University, Finland), Toni Ernvall (University of Turku, Finland) and Camilla Hollanti (Aalto University, Finland)

We3B : MIMO Wiretap Channel

Secure Degrees of Freedom for the MIMO Wiretap Channel with a Multiantenna Cooperative Jammer 626

Mohamed Nafea (The Pennsylvania State University, USA) and Aylin Yener (Pennsylvania State University, USA)

From Ordinary AWGN Codes to Optimal MIMO Wiretap Schemes 631

Anatoly Khina (Tel Aviv University, Israel), Yuval Kochman (The Hebrew University of Jerusalem, Israel) and

Ashish Khisti (University of Toronto, Canada)

Unshared Secret Key Cryptography : Achieving Shannon's Ideal Secrecy and Perfect Secrecy . . . 636

Shuiyin Liu (Monash University, Australia), Yi Hong (Monash University, Australia) and Emanuele Viterbo (Monash University, Australia)

The Role of Artificial Noise in Multi-Antenna Fading Wiretap Channels : Useful or Harmful? . . . 641

Ramanan Subramanian (University of South Australia & Institute of Telecommunications Research, Australia) and Ingmar Land (University of South Australia, Australia)

We3C : Relay Channels Strong Coordination over a Three-Terminal Relay Network 646

Matthieu Bloch (Georgia Institute of Technology & Georgia Tech Lorraine, France) and Joerg Klierer (New Jersey Institute of Technology, USA)

On the multiway relay channel with direct links 651

Anne Savard (CNRS / ENSEA / University Cergy-Pontoise, France) and Claudio Weidmann (CNRS / ENSEA / University Cergy-Pontoise, France)

Switched Local Schedules for Diamond Networks 656

Siddhartha Brahma (EPFL Switzerland, Switzerland), Ayan Sengupta (EPFL Switzerland, Switzerland) and Christina Fragouli (EPFL, Switzerland)

The Diversity Multiplexing Tradeoff of the Half-Duplex Relay Network 661

Sanjay Karmakar (North Dakota State University, USA)

Wireless-Powered Cooperative Communications via a Hybrid Relay 666

He Chen (The University of Sydney, Australia), Xiangyun Zhou (The Australian National University, Australia), Yonghui Li (University of Sydney, Australia), Peng Wang (The University of Sydney, Australia) and Branka Vucetic (The University of Sydney, Australia)
