

2010 IEEE Information Theory Workshop

(ITW 2010)

**Dublin, Ireland
30 August – 3 September 2010**



**IEEE Catalog Number: CFP10ITW-PRT
ISBN: 978-1-4244-8262-7**

TABLE OF CONTENTS

PLENARY TALK:

Abelian Varieties in Coding and Cryptography	1
<i>Ian F. Blake</i>	

CODING AND INFORMATION-THEORETIC METHODS IN CRYPTOGRAPHY:

Recent Results on Bent and Hyper-bent Functions and Their Link With Some Exponential Sums	6
<i>Sihem Mesnager</i>	
Boolean Functions Whose Restrictions are Highly Nonlinear	11
<i>Constanza Riera, Matthew G. Parker</i>	
Hecke Operators with odd Determinant and Binary Frameproof Codes Beyond the Probabilistic Bound?	16
<i>Hugues Randriam</i>	
Robust Parent-identifying Codes	21
<i>Alexander Barg, G. Robert Blakley, Grigory Kabatiansky, Cedric Tavernier</i>	
Coding Solutions for the Secure Biometric Storage Problem	25
<i>Davide Schipani, Joachim Rosenthal</i>	
Identification Codes in Cryptographic Protocols	29
<i>Julien Bringer, Herve Chabanne, Gerard Cohen, Bruno Kindarji</i>	

COOPERATION AND THROUGHPUT IN NETWORKS:

Cooperative Strategies for Relay-Aided Multi-Cell Wireless Networks with Backhaul	34
<i>Jinfeng Du, Ming Xiao, Mikael Skoglund</i>	
Throughput and Latency of Acyclic Erasure Networks with Feedback in a Finite Buffer Regime	39
<i>Nima Torabkhani, Badri N. Vellambi, Faramarz Fekri</i>	
Cooperative ARQs with Opportunistic Distributed Space-time Coding: Effective Protocols and Performance Analysis	44
<i>Hsin-Li Chiu, Sau-Hsuan Wu, Jin-Hao Li</i>	
On the Deterministic Multicast Capacity of Bidirectional Relay Networks	49
<i>M. Mokhtar, Y. Mohasseb, M. Nafie, H. El Gamal</i>	

LOW-DENSITY CODES:

Structured LDPC Codes from Permutation Matrices Free of Small Trapping Sets	54
<i>Dung Viet Nguyen, Bane Vasic, Michael Marcellin, Shashi Kiran Chilappagari</i>	
Quasi-cyclic Asymptotically Regular LDPC Codes	59
<i>David G. M. Mitchell, Roxana Smarandache, Michael Lentmaier, Daniel J. Costello</i>	
Irregular Repeat-accumulate-like Codes with Improved Error Floor Performance	64
<i>David F. Hayes, Sarah J. Johnson, Steven R. Weller</i>	
Lossy Source Compression of Non-uniform Binary Sources Using GQ-LDGM Codes	69
<i>Lorenzo Cappellari</i>	

COMMUNICATION WITH SECRECY SONCRAINTS:

Strong Secrecy for Erasure Wiretap Channels	74
<i>Ananda T. Suresh, Arunkumar Subramanian, Andrew Thangaraj, Matthieu Bloch, Steven W. McLaughlin</i>	
Wiretap Channel with Shared Key	79
<i>Wei Kang, Nan Liu</i>	
Multiple Access Wiretap Channels with Strong Secrecy	84
<i>Mohammad Hossein Yassaee, Mohammad Reza Aref</i>	

Secure Type-based Multiple Access: Transmission Strategy and Analysis for Perfect Secrecy	89
<i>Hyongsuk Jeon, Daesung Hwang, Hyuckjae Lee, Jeongseok Ha, Jinho Choi</i>	

COMMUNICATION THEORY 1:

Exact PWM Representation of Bandlimited Signals	94
<i>Jing Huang, Krishnan Padmanabhan, Oliver M. Collins</i>	
Fading Channels with 1-bit Output Quantization: Optimal Modulation, Ergodic Capacity and Outage Probability	99
<i>Stefan Krone, Gerhard Fettweis</i>	
On Optimum Communication Cost for Joint Compression and Dispersive Information Routing	104
<i>Kumar Viswanatha, Emrah Akyol, Kenneth Rose</i>	
On the Secure Outage Performance for Wireless Multicasting through Slow Fading Channels	109
<i>Md. Zahurul I. Sarkar, Tharmalingam Ratnarajah</i>	

CODING FOR MEMORIES:

Dense Error-correcting Codes in the Lee Metric	114
<i>Tuvi Etzion, Alexander Vardy, Eitan Yaakobi</i>	
On The Parallel Programming of Flash Memory Cells	119
<i>Eitan Yaakobi, Anxiao Andrew Jiang, Paul H. Siegel, Alexander Vardy, Jack K. Wolf</i>	
Efficient Two-write WOM-codes	124
<i>Eitan Yaakobi, Scott Kaysner, Paul H. Siegel, Alexander Vardy, Jack K. Wolf</i>	
Constrained Codes for Phase-change Memories	129
<i>Anxiao Andrew Jiang, Jehoshua Bruck, Hao Li</i>	

COMMUNICATION WITH MULTIPLE ANTENNAS:

An Achievable Rate for the MIMO Individual Channel	134
<i>Yuval Lomnitz, Meir Feder</i>	
How to Achieve the Optimal DMT of Selective Fading MIMO Channels?	139
<i>Lina Mroueh, Jean-Claude Belfiore</i>	
A New Full-diversity Criterion and Low-complexity STBCs with Partial Interference Cancellation Decoding	144
<i>Lakshmi Prasad Natarajan, B. Sundar Rajan</i>	
Information-theoretic Performance Analysis of LMS MIMO Communications	149
<i>Giuseppa Alfano, Antonio De Maio, Antonia M.Tulino</i>	
Coding for the MIMO ARQ Block-fading Channel with Imperfect Feedback and CSIR	154
<i>A. Taufiq Asyhari, Albert Guillen i Fabregas</i>	

SECURE COMMUNICATION:

Stopping Sets for Physical-layer Security	159
<i>Willie K. Harrison, Joao Almeida, Demijan Klinc, Steven W. McLaughlin, Joao Barros</i>	
Non-systematic Codes for Physical Layer Security	164
<i>Marco Baldi, Marco Bianchi, Franco Chiaraluce</i>	
Low-complexity Wire-tap Codes with Security and Error-correction Guarantees	169
<i>Yuval Cassuto, Zvonimir Bandic</i>	
An Extension of Massey Scheme for Secret Sharing	174
<i>Romar dela Cruz, Annika Meyer, Patrick Sole</i>	

POLAR CODES:

Universal Source Polarization and Sparse Recovery	179
<i>Emmanuel Abbe</i>	
Secrecy-achieving Polar-coding	184
<i>Eran Hof, Shlomo Shamai</i>	

On Speed of Channel Polarization	189
<i>Toshiyuki Tanaka</i>	

POLAR AND LDPC CODES:

Polar Coding for Reliable Communications over Parallel Channels	194
<i>Eran Hof, Igal Sason, Shlomo Shamai</i>	
Non-binary Polar Codes using Reed-solomon Codes and Algebraic Geometry Codes	199
<i>Ryuhei Mori, Toshiyuki Tanaka</i>	
On LP Decoding of Polar Codes	204
<i>Naveen Goela, Satish Babu Korada, Michael Gastpar</i>	

COMMUNICATION THEORY 2:

On the Capacity Region of the Degraded Z Channel	209
<i>Sadaf Salehkalaibar, Mohammad Reza Aref</i>	
Bit-interleaved Coded Modulation with Shaping	214
<i>Albert Guillen I. Fabregas, Alfonso Martinez</i>	
Achievable Rate Regions for Dirty Tape Channels and "Joint Writing on Dirty Paper and Dirty Tape"	219
<i>Reza Khosravi-Farsani, Bahareh Akhbari, Mohammad Reza Aref</i>	
Coding for the Z Channel With a Digital Relay Link	224
<i>Hieu T. Do, Tobias J. Oechtering, Mikael Skoglund</i>	

ALGEBRAIC CODES:

On the Degree of the Inverse of Quadratic Permutation Polynomial Interleavers	229
<i>Eva Suvitte, Jyrki Lahtonen</i>	
The Projective Kerdock Code	234
<i>M. M. Nastasescu, A. R. Calderbank</i>	
Information sets for Abelian Codes	239
<i>Jose Joaquin Bernal, Juan Jacobo Simon</i>	
Additive Codes over $Z_2 \times Z_4$	244
<i>Joaquim Borges, Cristina Fernandez-Cordoba, Steven T. Dougherty</i>	

GRAPHICAL MODELS AND DECODING:

Tail-biting Products Trellises, the BCJR-construction and their Duals	247
<i>Heide Gluesing-Luerssen, Elizabeth Weaver</i>	
Valiant Transform of Forney Graphs	252
<i>Ali Al-Bashabsheh, Yongyi Mao</i>	
An Algebraic View to Gradient Descent Decoding	257
<i>M. Borges Quintana, M. A. Borges Trenard, I. Marquez-Corbella, E. Martinez-Moro</i>	
The Euclidean Algorithm for Generalized Minimum Distance Decoding of Reed-solomon Codes	261
<i>Sabine Kampf, Martin Bossert</i>	
Universal A Posteriori Metrics Game	266
<i>Emmanuel Abbe, Rethnakaran Pulikkoonattu</i>	

CODING AND DECODING:

Computation of the Robust Symmetrical Number System Dynamic Range	271
<i>Brian L. Luke, Phillip E. Pace</i>	
Properties of Optimal Prefix-free Machines as Instantaneous Codes	276
<i>Kohtaro Tadaki</i>	
Group Permutable Constant Weight Codes	281
<i>Oscar Moreno, Jose Ortiz-Ubarri</i>	

Codes from Graphs Related to the Categorical Product of Triangular Graphs and K_n	286
<i>Khumbo Kumwenda, Eric Mwambene</i>	

INTERFERENCE CHANNELS:

On Achievable Rates for Classes of Non-linear Deterministic Interference Channels	291
<i>Amin Jafarian, Sriram Vishwanath</i>	
Outer Bounds for the Interference Channel with a Cognitive Relay	296
<i>Stefano Rini, Daniela Tuninetti, Natasha Devroye</i>	
Capacity Regions for Some Classes of Causal Cognitive Interference Channels With Delay	301
<i>Mahtab Mirmohseni, Bahareh Akhbari, Mohammad Reza Aref</i>	
Sum Capacity of K User Gaussian Degraded Interference Channels	306
<i>Jubin Jose, Sriram Vishwanath</i>	
The Capacity Region of the Interference Channel with a Relay in the Strong Interference Regime Subject to Phase Fading	311
<i>Ron Dabora</i>	

PLENARY TALK:

Local Computation in Codes	316
<i>Tali Kaufman</i>	

LDPC CODES:

Improved Linear Programming Decoding and Bounds on the Minimum Distance of LDPC Codes	321
<i>David Burshtein, Idan Goldenberg</i>	
A Graphical Model for Computing the Minimum Cost Transposition Distance	326
<i>Farzad Farnoud, Chien-Yu Chen, Olgica Milenkovic, Navin Kashyap</i>	
Coupled Graphical Models and their Thresholds	331
<i>S. Hamed Hassani, Nicolas Macris, Ruediger Urbanke</i>	
Characterization of Graph-cover Pseudocodewords of Codes over F_3	336
<i>Vitaly Skachek</i>	

WIRELESS NETWORKS:

Network-level Cooperative Protocols for Wireless Multicasting: Stable Throughput Analysis and Use of Network Coding	341
<i>Anthony Fanous, Anthony Ephremides</i>	
The Benefits from Simultaneous Transmission and Reception in Wireless Networks	346
<i>P. C. Weeraddana, M. Codreanu, M. Latva-aho, Anthony Ephremides</i>	
The Collection Channel In a Wireless Sensor Network	351
<i>Bryan Larish, George Riley</i>	
Fireworks: A Random Linear Coding Scheme for Distributed Storage in Wireless Sensor Networks	356
<i>Dejan Vukobratovic, Cedomir Stefanovic, Vladimir Stankovic</i>	

ALGEBRAIC CODES AND SEQUENCES:

Unimodular Lattices for the Gaussian Wiretap Channel	361
<i>Jean-Claude Belfiore, Patrick Sole</i>	
Generalized Frobenius Extensions of Finite Rings and Trace Functions	366
<i>Marcus Greferath, Alexandr Nechaev</i>	
The Enumeration of Costas Arrays of Order 28	371
<i>Konstantinos Drakakis, Francesco Iorio, Scott Rickard</i>	

ESTIMATION AND PORTFOLIO THEORY:

The Confidence Interval of Entropy Estimation through a Noisy Channel	376
<i>Siu-Wai Ho, Terence Chan, Alex Grant</i>	
On Conditions for Linearity of Optimal Estimation	381
<i>Emrah Akyol, Kumar Viswanatha, Kenneth Rose</i>	
On Thresholds for Robust Goodness-of-fit Tests	386
<i>Jayakrishnan Unnikrishnan, Sean Meyn, Venugopal V. Veeravalli</i>	
Universal Portfolio Algorithms in Realistic-outcome Markets	390
<i>Ami Tavorly, Meir Feder</i>	

INFORMATION THEORETIC METHODS:

Error Exponents in Multiple Hypothesis Testing for Arbitrarily Varying Sources	395
<i>Naira M. Grigoryan, Ashot N. Harutyunyan</i>	
Capacity of a Noisy Function	400
<i>Francois Simon</i>	
Source Coding With Common Reconstruction and Action-dependent Side Information	405
<i>Kittipong Kittichokechai, Tobias J. Oechtering, Mikael Skoglund</i>	
Information-theoretical Analysis of Private Content Identification	410
<i>S. Voloshynovskiy, O. Koval, F. Beekhof, F. Farhadzadeh, T. Holotyak</i>	

QUANTUM INFORMATION PROCESSING:

Quantum Channel Capacities	415
<i>Graeme Smith</i>	
Stabilizer Subsystem Codes with Spatially Local Generators	420
<i>Sergey Bravyi</i>	
Quantum Erasure-correcting Codes and Percolation on Regular Tilings of the Hyperbolic Plane	425
<i>Nicolas Delfosse, Gilles Zemor</i>	

NETWORK CODING:

Rotate-and-add Coding: A Novel Algebraic Network Coding Scheme	430
<i>Alireza Keshavarz-Haddad, Mohammad Amir Khojastepour</i>	
On the Delay Advantage of Coding in Packet Erasure Networks	435
<i>Theodoros K. Dikaliotis, Alexandros Dimakis, Tracey Ho, Michelle Effros</i>	
Orbit Codes - A New Concept in the Area of Network Coding	440
<i>Anna-Lena Trautmann, Felice Manganiello, Joachim Rosenthal</i>	
On Secure Network Coding with Unequal Link Capacities and Restricted Wiretapping Sets	444
<i>Tao Cui, Tracey Ho, Joerg Kliewer</i>	

QUANTUM INFORMATION PROCESSING (CON'D):

On Encoders for Quantum Convolutional Codes	449
<i>Markus Grassl, Martin Roetteler</i>	
A Renormalization Group Decoding Algorithm for Topological Quantum Codes	454
<i>Guillaume Duclos-Cianci, David Poulin</i>	
Topological Color Codes over Higher Alphabet	459
<i>Pradeep Sarvepalli</i>	

CODING AND CAPACITY OF NETWORKS:

Multi-source Operator Channels: Efficient Capacity-achieving Codes	464
<i>Hongyi Yao, Theodoros K. Dikaliotis, Sidharth Jaggi, Tracey Ho</i>	
Reduced-state Decoding in Two-way Relay Networks With Physical-layer Network Coding	469
<i>Duc To, Jinho Choi</i>	

Approximate Capacity of a Class of Multi-source Gaussian Relay Networks	474
<i>Sang-Woon Jeon, Sae-Young Chung, Syed A. Jafar</i>	
Gaussian Diamond Network with Adversarial Jammer	479
<i>Soheil Mohajer, Suhas N. Diggavi</i>	

PLENARY TALK:

Applications of Semidefinite Programming to Coding Theory	484
<i>Christine Bachoc</i>	

CHANNEL UNCERTAINTY:

Every Channel with Time Structure has a Capacity Sequence	489
<i>Rudolf Ahlswede</i>	
Coding Against Myopic Adversaries	490
<i>Anand D. Sarwate</i>	
A Multi-hop Multi-source Algebraic Watchdog	495
<i>MinJi Kim, Muriel Medard, Joao Barros</i>	
Author Index	