

2010 International Symposium on Information Theory and its Applications

(ISITA 2010)

**Taichung, Taiwan
17 - 20 October 2010**

Pages 1 - 536



**IEEE Catalog Number: CFP1005E-PRT
ISBN: 978-1-4244-6016-8**

Session Index

ES1-Mo-1: LDPC Codes I

ES2-Mo-1: MIMO I

LS2-Mo-1: Cryptography I

CW-Mo-1: Source Coding I

Au-Mo-1: Stochastic Processes/Pattern Recognition

ES1-Mo-2: Error-Control Coding I

ES2-Mo-2: Cooperative Communications I

LS2-Mo-2: Cryptography II

CW-Mo-2: Signal Processing for Communications

Au-Mo-2: Video/Image Coding

ES1-Mo-3: Error-Control Coding II

ES2-Mo-3: OFDM I

LS2-Mo-3: Digital Watermarking

CW-Mo-3: Data Networks

Au-Mo-3: Cooperative MIMO

ES1-Tu-1: LDPC Codes II

ES2-Tu-1: Multiuser Information Theory I

LS2-Tu-1: Cryptography III

CW-Tu-1: Shannon Theory I

Au-Tu-1: Constrained Coding

ES1-Tu-2: LDPC Codes III

ES2-Tu-2: MIMO II

LS2-Tu-2: Cryptography IV

CW-Tu-2: Source Coding II

Au-Tu-2: Signal Processing

ES1-Tu-3: Coding Performance

ES2-Tu-3: OFDM II

LS2-Tu-3: Cryptography V

CW-Tu-3: Multiuser Information Theory II

Au-Tu-3: Performance Evaluation

ES1-We-1: Decoding

LS2-We-1: Cryptography VI

CW-We-1: Shannon Theory II

Au-We-1: Sequences

ES1-We-2: Error-Control Coding III

ES2-We-2: MIMO III

LS2-We-2: Cryptography VII

CW-We-2: Cognitive and Software Radio

Au-We-2: Cooperative Communications II

ES1-We-3: RS/AG Codes

ES2-We-3: Multiuser Information Theory III

LS2-We-3: Quantum Information

CW-We-3: OFDM PAPR

ES1-Mo-1: LDPC Codes I

Good High-Rate π -Rotation LDPC Codes Based on Novel Puncturing Techniques 1
Rich Echard, Shih-Chun Chang

Low-Density Parity-Check Accumulate Codes 7
Chung-Li Wang, Shu Lin

Adaptive Quantization for Low-Density-Parity-Check Decoders 13
Cha-Hao Chung, Yeong-Luh Ueng, Ming-Che Lu, Mao-Chao Lin

Error-Trellis State Complexity of LDPC Convolutional Codes Based on Circulant Matrices 19
Masato Tajima, Koji Okino, Takashi Miyagoshi

ES2-Mo-1: MIMO I

Approximately Universal MIMO Diversity Embedded Codes 25
Hsiao-feng (Francis) Lu

MIMO MFSK receivers using FDE and MLD on quasi-static frequency selective fading channels 31
Kenji NAKAYAMA, Yasunori IWANNAMI, Eiji OKAMOTO

Lattice-Reduction Aided HNN for Vector Precoding 37
Vesna Gardašević, Ralf R. Müller, Daniel J. Ryan, Lars Lundheim, Geir E. Øien

A Family of Cyclic Division Algebra Based Fast-Decodable 4x2 Space-Time Block Codes 42
Roope Vehkalahti, Camilla J. Hollanti, Jyrki Lahtonen

LS2-Mo-1: Cryptography I

Direct Biometric Verification Schemes with Gaussian Data	48
<i>Vladimir B. Balakirsky, A. J. Han Vinck</i>	
Fundamental Limits for Biometric Identification with a Database Containing Protected Templates	54
<i>Tanya Ignatenko, Frans M.J. Willems</i>	
A Geometric View of Mutual Information: Application to Anonymity Protocols	60
<i>Sami Zhioua</i>	
Realizing and Evaluating Mutual Anonymity in P2P Networks	66
<i>Chigusa Kawashima, I. G. B. Baskara Nugraha, Hiroyoshi Morita, Todorka Alexandrova</i>	

CW-Mo-1: Source Coding I

On the Adaptive Antidictionary Code Using Minimal Forbidden Words with Constant Lengths	72
<i>Takahiro Ota, Hiroyoshi Morita</i>	
On Coding for Source with Infinitesimal Time Slots	78
<i>Mikihiko Nishiara</i>	
Using Synchronization Bits to Boost Compression by Substring Enumeration	82
<i>Danny Dubé</i>	
On Coding for Nonbinary Sources with Side Information at the Decoder	88
<i>Shohei Iwata, Toshihiro Hattori, Motohiko Isaka</i>	

Au-Mo-1: Stochastic Processes/Pattern Recognition

Stationary Sequences and Stable Sampling	94
<i>Juan Miguel Medina, Bruno Cernuschi Friás</i>	
Approximating Discrete Probability Distributions with Causal Dependence Trees	100
<i>Christopher J. Quinn, Todd P. Coleman, Negar Kiyavash</i>	
English And Taiwanese Text Categorization Using N-gram Based on Vector Space Model	106
<i>Makoto Suzuki, Naohide Yamagishi, Yi-Ching Tsai, Takashi Ishida, Masayuki Goto</i>	
A note on model selection for small sample regression	112
<i>Masanori KAWAKITA, Yoko OIE, Jun'ichi TAKEUCHI</i>	

ES1-Mo-2: Error-Control Coding I

Proper self-complementary codes	118
<i>Torleiv Kløve, Somaye Yari</i>	
Computing the Degree of a Boolean Function from its Support	123
<i>Joan-Josep Climent, Francisco García, Verónica Requena</i>	

BER Analysis for MIMO BICM-ID Assuming Finite Precision of Extrinsic LLR 129
Chien-Yi Wang, I-Wei Lai, Tzi-Dar Chiueh, Gerd Ascheid, Heinrich Meyr

Upper bounds on the Average Probability of Undetected Error for the Ensembles of both Product and Concatenated Codes 135
Toshihisa Nishijima, Kin-ichiroh Tokiwa

Practical Design and its Evaluations for Nested Transmit Diversity 139
Takashi HAYASHI, Koji ISHII, Shigeaki OGOSE

ES2-Mo-2: Cooperative Communications I

Improving Error Performance of Joint Channel and Network Coding in Multiple Access Relay Channel 145
E. Kurniawan, S. Sun, K. Yen, K. F. E. Chong

Split-Extended LDPC codes for coded cooperation 151
Valentin Savin

Joint Relay Selection and Link Adaptation for Distributed Beamforming in Regenerative Cooperative Network 157
Wei Yang, Lihua Li, Gang Wu, Haifeng Wang

Performance Analysis and Optimal Power Allocation for Hybrid Incremental Relaying 163
Jaeyoung Lee, Sung-il Kim, Jun Heo

Modeling of DF Behavior and SNR Evaluation for Multinode Cooperation System with Adaptive Modulation under Different Diversity Combining Strategies 169
Shi-Yong Lee, Chia-Chun Chang, Min-Kuan Chang

LS2-Mo-2: Cryptography II

Secrecy Gain: a Wiretap Lattice Code Design 174
Jean-Claude Belfiore, Frédérique Oggier

Secure rate-adaptive reconciliation 179
David Elkouss, Jesús Martínez-Mateo, Vicente Martin

Secret Key Establishment over a Pair of Independent Broadcast Channels 185
Hadi Ahmadi, Reihaneh Safavi-Naini

New Results on Secret Key Establishment over a Pair of Broadcast Channels 191
Hadi Ahmadi, Reihaneh Safavi-Naini

Secret Key Rate Region of Multiple Access Channel Model 197
Somayeh Salimi, Mahmoud Salmasizadeh, Mohammad Reza Aref

CW-Mo-2: Signal Processing for Communications

Wireless Relay Networks Using Multiple Frequency Bands 203

Toshiyuki Kikkawa, Yukitoshi Sanada

Performance Analysis of Equalization and Interference Cancellation by Adaptive Digital Filter for UWB-IR System inside a Vehicle 209

Aya Inami, Chika Sugimoto, Ryuji Kohno

A Study on Estimating Implanted Devices Using Image Information and Ranging System Using UWB Radio 215

Hiroshi Takayama, Chika Sugimoto, Ryuji Kohno

A Novel Positioning Estimation Method with the Correlation between Sensor's Data 220

Yuuki MATSUURA, Koji ISHII, Shigeaki OGOSE

Iterative Algorithm using Particle Filter for Positioning in NLOS Environment 225

Koji ENDA, Ryuji KOHNO

Au-Mo-2: Video/Image Coding

Probabilistic Search of Nonbinary LDPC Codes for Distributed Video Coding 231

Haruhiko Kaneko

Selective Multiple Reference Frames Motion Estimation for H.264/AVC Video Coding 237

Chih-Chung Tsui, Yu-Ming Lee, Yinyi Lin

Spectral Entropy-Based Bit Allocation 243

Malavika Bhaskaranand, Jerry D. Gibson

Practical Estimation of Adaptive Correlation Noise Model for Distributed Video Coding 249

Tsung-Han Tsai, Chang-Ming Lee, Wen-Nung Lie

Iterative Prior-knowledge-based Image Reconstruction Algorithms 255

Hsin M. Shieh, Jin-Gui Li, Yu-Ching Hsu, Meng-Chi Ye, Dong G. Lee

ES1-Mo-3: Error-Control Coding II

Turbo Equalization and an M-BCJR Algorithm for Strongly Narrowband Intersymbol Interference 261

John B. Anderson, Adnan Prlja

Adaptive Single-Trial Error/Erasur e Decoding of Binary Codes 267

Christian Senger, Vladimir R. Sidorenko, Steffen Schober, Martin Bossert, Victor V. Zyablov

More on General Error Locator Polynomials for a Class of Binary Cyclic Codes 273

Chong-Dao Lee, Yaotsu Chang, Trieu-Kien Truong, Yan-Haw Chen

Efficient decoding algorithm for constant composition codes 278

Jen-chum Chang, I-te Tsai, Hsin-lung Wu

ES2-Mo-3: OFDM I

A Robust Cross Coding Scheme for OFDM Systems	282
<i>Xiaoying Shao, Cornelis H. Slump</i>	
A Modulation Classification Using Amplitude Moments in OFDM systems	288
<i>Daisuke Shimbo, Ikuo Oka</i>	
Time Domain Feedback Equalizer for Fast Fading Channel in OFDM with Scattered Pilot	294
<i>Yutaro Nakagawa, Yukitoshi Sanada</i>	
Novel Lifetime-aware Bit and Power Allocation in OFDM Systems	298
<i>Shi-Yong Lee, Chia-Chun Chang, Min-Kuan Chang</i>	

LS2-Mo-3: Digital Watermarking

An Audio Watermarking Method by Using Automatic Music Transcription Information	303
<i>Harumi Murata, Akio Ogihara, Motoi Iwata, Akira Shiozaki</i>	
Digital Watermarking Method for Tamper Detection and Recovery of JPEG Images	309
<i>Motoi Iwata, Tomoki Hori, Akira Shiozaki, Akio Ogihara</i>	
A Scheme of Digital Watermarking for 3-D Models using Correlation Method in Polar Coordinate System	315
<i>Shouta Sakaino, Hiromu Koda</i>	
A Simple Detection Scheme of LSB Steganography Based on Statistics of Image Difference Signal	320
<i>Tadakazu Sakakura, Akira Hayashi</i>	
A New Method to Reduce the Probability of Detection Errors for a Digital Watermark Using Complementary Decoding Algorithms and Minimum Weight Codewords of Linear Code	326
<i>Tetsushi Masuno, Takuya Kusaka, Toru Fujiwara</i>	

CW-Mo-3: Data Networks

Longest Queue First in Round-Robin Matching for Input-Queued Switches	332
<i>Jan-Ray Liao, Pin-Hsuan Wu</i>	
Optimal Network Planning in Robust Two Site's Communication	337
<i>Shin-Guang Chen</i>	
Directed Information and the NRL Network Pump	343
<i>Siva K. Gorantla, Sachin Kadloor, Todd P. Coleman, Negar Kiyavash, Ira S. Moskowitz, Myong H. Kang</i>	
Continuum Percolation in the Intrinsically Secure Communications Graph	349
<i>Pedro C. Pinto, Moe Z. Win</i>	

Au-Mo-3: Cooperative MIMO

Diamond Relay Network under Rayleigh Fading: On-off Power Control and Outage-Capacity Bound 355
Mingjun Dai, Ping Hu, Chi Wan Sung

Diversity Analysis of the Best Relay Selection for Soft-Decision-and-Forward Cooperative Network 361
Kyoung-Young Song, Jaehong Kim, Jong-Seon No, Habong Chung

Analysis Performance of Decode-and-Forward scheme in Distributed MIMO Repeater System 365
Pham Thanh Hiep, Ryuji Kohno

Efficient Space-Time Block Codes for Cooperative MIMO Communications 371
Y. Nasser, J.-F. Héland

A Non-Coherent AF Scheme for Two-Way Wireless Relay Networks based on Packings in Grassmann Manifolds 377
Zoran Utkovski, Yao Cheng, Juergen Lindner

ES1-Tu-1: LDPC Codes II

Circulant Decomposition: Cyclic, Quasi-Cyclic and LDPC Codes 383
Qin Huang, Qiuju Diao, Shu Lin

Importance Sampling for LDPC Codes Based on Optimal Simulation Probability Density Function 389
Takakazu SAKAI, Koji SHIBATA

An Iterative Decoding Algorithm for Rate-Compatible Punctured Low-Density Parity-Check Codes of High Coding Rates 394
Gou Hosoya, Hideki Yagi, Manabu Kobayashi

Optimized puncturing distributions for irregular non-binary LDPC codes 400
Matteo Gorgoglione, Valentin Savin, David Declercq

ES2-Tu-1 : Multiuser Information Theory I

Körner-Marton Theorem for Binary Modulo-Two Sum Problem from Canonical Equations (Invited Paper) 406
Richard E. Blahut, Soumya Jana

On Arbitrarily Varying Bidirectional Broadcast Channels with Constraints on Input and States 410
Rafael F. Wyrembelski, Igor Bjelaković, Holger Boche

The Compound MAC With Common Message and Partial Channel State Information 416
Moritz Wiese, Holger Boche, Igor Bjelaković

Diversity-Multiplexing Tradeoff Analysis of Multi-source Multi-relay Coded Networks 422
Chao Wang, Ming Xiao, Mikael Skoglund

LS2-Tu-1: Cryptography III

A Knapsack Cryptosystem Based on Multiple Knapsacks 428
Kunikatsu Kobayashi, Kohtaro Tadaki, Masao Kasahara, Shigeo Tsujii

A New Construction Method of Knapsack PKC Using Linear Transformation and Chinese Remainder Theorem 433
Yasuyuki Murakami

On the Critical Density Associated with the Matrix Type Knapsack Cryptosystem 437
Akira Hayashi

Improvement of the Low Rank Attack 441
Masahito Gotaishi

CW-Tu-1: Shannon Theory I

On Kolmogorov-Nagumo averages and Nonextensive entropy 446
Ambedkar Dukkipati

Error Exponents of Discrete Memoryless Channels and AWGN Channels with Noisy Feedback 452
Akari Sato, Hirosuke Yamamoto

Data Transmission in the Presence of Noisy Channel State Feedback and Outage Probability Constraint 458
Behrooz Makki, Thomas Eriksson

On the Capacity Region of a Class of Z Channels with Cooperation 464
Sadaf Salehkalaibar, Mohammad Reza Aref

Au-Tu-1: Constrained Coding

High-Rate Maximum Runlength Constrained Coding Schemes Using Base Conversion 469
Kees A. Schouhamer Immink

A Prefix-free Coding for Finite-State Noiseless Channels with Small Coding Delay 473
Ken-ichi Iwata, Takuya Koyama

Syndrome Former Trellis Construction for Punctured Convolutional Codes 478
Jan Geldmacher, Juergen Goetze

On Soft Iterative Decoding For Ternary Recording Systems With RLL Constraints 484
Shih-Kai Lee, Hsin-Yi Chen, Mao-Chao Lin, Tien-Hui Chen

ES1-Tu-2: LDPC Codes III

Recovering Synchronization with Iterative Decoders: LDPC Codes 490
Raúl Martínez-Noriega, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi

Optimization of Memory Utilization for Partially Parallel QC-LDPC Decoder 496
Tsung-Che Wu, Yao-Wen Hu, Chang-Ming Lee

A Message-Passing Decoding Algorithm for q -ary LDPC Codes With Low-Complexity 501
Chao-Yu Chen, Qin Huang, Chi-chao Chao, Shu Lin

A New Construction of Irregular LDPC Convolutional Codes with Cycle Removal 507
Chi-Jen Wu, Chung-Hsuan Wang, Chi-chao Chao

Detailed Evaluation of Error Floors of LDPC Codes Using the Probabilistic Algorithm 513
Masanori Hiroto, Masakatu Morii

ES2-Tu-2: MIMO II

An Achievable Rate of Large Block-Fading MIMO Systems with No CSI via Successive Decoding 519
Keigo Takeuchi, Ralf R. Müller, Mikko Vehkaperä, Toshiyuki Tanaka

MIMO Block-Fading Channels with Mismatched CSIR 525
A. Taufiq Asyhari, Albert Guillén i Fàbregas

MIMO Systems with Mutual Coupling: How Many Antennas to Pack into Fixed-Length Arrays? 531
Shuo Shen, Matthew R. McKay, Ross D. Murch

Some Simple Observations on MISO Codes 537
Roope Vehkalahti, Camilla Hollanti, Jyrki Lahtonen, Hsiao-feng (Francis) Lu

MIMO Broadcast Channel Rate Region with Linear Precoding at High SNR without Full Multiplexing 542
Paul de Kerret, Michael Joham, Wolfgang Utschick, Rudolf Mathar

LS2-Tu-2 : Cryptography IV

An ANFIS-IDS against Deauthentication DOS Attacks for a WLAN 548
Jeich Mar, Yow-Cheng Yeh, I-Fan Hsiao

A User Authentication Scheme Using Multiple Passphrases and Its Arrangement 554
Hirota Tazawa, Takashi Katoh, Bhed Bahadur Bista, Toyoo TAKATA

Anti-Phishing Mutual Authentication Using the Visual Secret Sharing Scheme 560
Kai Zhao, Yuichi Kaji

De-synchronization Attack on RFID Authentication Protocols 566
N.W. Lo, Kuo-Hui Yeh

How to Distinguish On-line Dictionary Attacks and Password Mis-typing in Two-Factor Authentication 571
Yasunori Onda, SeongHan Shin, Kazukuni Kobara, Hideki Imai

CW-Tu-2: Source Coding II

Relations between Universal FV and FF Source Codes 577
Shigeaki KUZUOKA

On Embeddings of Shifts of Finite Type into the Golden-Mean-Dyck Shift <i>Hiroshi Fujisaki</i>	583
Optimality of LDGM-LDPC Compound Codes for Lossy Compression of Binary Erasure Source <i>Grégory Demay, Vishwambhar Rathi, Lars K. Rasmussen</i>	589
The Minimum Achievable Redundancy Rate of Fixed-to-Fixed Length Source Codes for General Sources <i>Mitsuharu Arimura, Ken-ichi Iwata</i>	595
Joint JPEG-Block Coding With Expurgating Trellis for Wireless Robust Image Transmission <i>Jyun-Jie Wang, Houshou Chen, Zhin-Han Dai, Hsinying Liang</i>	601
 Au-Tu-2 : Signal Processing	
Implementation of Finite Impulse Response Systems Using Rotation Structures <i>Krzysztof Wawryn, Robert T. Wirski, Bogdan Strzeszewski</i>	606
A Design Method for IIR Digital Filters with Variable Stopband Using Semidefinite Programming <i>Nanako Ubayama, Toma Miyata, Naoyuki Aikawa</i>	611
Synthesis of Orthogonal Roesser Model for Two-Dimensional FIR Filters <i>Robert T. Wirski</i>	616
The optimum approximate reconstruction of a signal from the discrete sample values of the prescribed multiple waves <i>Yuichi Kida, Takuro Kida</i>	621
Development of a new numerical solution of inhomogeneous linear partial differential equations with many independent variables <i>Yuichi Kida, Takuro Kida</i>	627
 ES1-Tu-3 : Coding Performance	
Improved Decoding of Shannon-Kotel'nikov Mappings <i>Matthias Rüngeler, Birgit Schotsch, Peter Vary</i>	633
Pulse Interference Mitigation Techniques for QPSK and QAM using Viterbi Decoding <i>Yu Morishima, Ikuo Oka, Shingo Ata</i>	639
Performance Evaluation of Go-Back-i-symbol ARQ Scheme Applicable to Meteor Burst Communications <i>Shinsuke NAGATA, Kaiji MUKUMOTO, Tadahiro WADA, Koji ISHIBASHI</i>	644
Bounds on End-to-End Performance of Networks Employing Erasure Control Coding <i>Xiao-Hong Peng</i>	650
 ES2-Tu-3: OFDM II	
User/Sampling Point Selection Algorithm in Multiuser MIMO-OFDM with Fractional Sampling <i>Kenta Eguchi, Haruki Higuchi, Yukitoshi Sanada</i>	656

Low-Complexity Sampling Point Selection in OFDM Receiver with Fractional Sampling <i>Eisuke Sakai, Haruki Nishimura, Mamiko Inamori, Yukitoshi Sanada, Mohammad Ghavami</i>	662
A Novel CRC Based Error Correction Scheme in OFDM/OFDMA Wireless Networks <i>Chen, Chia-Yao, Jia, Wen-Kang, Chen, Yaw-Chung</i>	668
Bidirectional Decision Feedback Equalization for Mobile MIMO-OFDM Systems <i>Rih-Lung Chung, Chin-Wen Chang, Jeng-Kuang Hwang</i>	673

LS2-Tu-3: Cryptography V

Two Generalizations of a Coding Theorem for a (2,2)-Threshold Scheme with a Cheater <i>Hiroki Koga</i>	678
A Secure Authentication System Based on Variable-Length Codes <i>Ulrich Speidel, T. Aaron Gulliver</i>	684
A Low Complexity Authentication Protocol Based on Pseudorandomness, Randomness and Homophonic Coding <i>Miodrag Mihaljević, Hajime Watanabe, Hideki Imai</i>	690
Product Perfect Z_2Z_4 -linear codes in Steganography <i>Josep Rifà, Lorena Ronquillo</i>	696

CW-Tu-3 : Multiuser Information Theory II

A Theoretical Framework for Capacity-Achieving Multi-User Waterfilling in OFDMA <i>Simon Göertzen, Anke Schmeink</i>	702
The Performance of QPSK in Low-SNR Interference Channels <i>Moritz Wiese, Frederic Knabe, Johannes Georg Klotz, Aydin Sezgin</i>	708
On the Rate Distortion Region of Gaussian Multiterminal Source Coding <i>Yasutada Oohama</i>	714
The Capacity of a Class of Linear Deterministic Relay Networks <i>S. M. Hossein Tabatabaei Yazdi, Mohammad Reza Aref</i>	720
Double-Directional Information Azimuth Spectrum and Relay Network Tomography for a Decentralized Wireless Relay Network <i>Yifan Chen, Chau Yuen, Yong Huat Chew</i>	726

Au-Tu-3 : Performance Evaluation

O&7PSK MODULATION AND ITS BIT ERROR RATE PERFORMANCE <i>Shin'ichi Koike, Seiichi Noda</i>	732
Theoretical Analysis of M-CSK/CDMA system in optical wireless channel <i>Yusuke Kozawa, Hiromasa Habuchi</i>	738

Inband and Outband Spectrum Analysis of the BFDm and BFDm/OQAM Signals with Truncated Gaussian Pulses 743

Bayarpurev Mongol, Takaya Yamazato, Masaaki Katayama

A New Bit-Labeling for Trellis-Shaped PSK with Improved PAPR Reduction Capability 747

Yuuki Nishino, Makoto Tanahashi, Hideki Ochiai

Signal Analysis and Classification of Digital Communication Signal Using Higher Order Time-Frequency Analysis Techniques 752

Jo Lynn Tan, Ahmed Zuri bin Sha'ameri, Yen Mei Chee

ES1-We-1 : Decoding

Path Deletions for Finite Stack-Size Sequential-Type Decoding Algorithms 757

Chen-Yi Wang, Shin-Lin Shieh, Po-Ning Chen, Yungshiang S. Han

Theoretical Analysis of Bit Error Probability for 4-State Recursive Systematic Convolutional Code with Max-Log MAP Decoding 762

Hideki Yoshikawa, Yoshitake Kawadai

Theoretical Analysis of Bit Error Probability for Log-MAP Decoding 767

Hideki Yoshikawa

Adaptive Recursive MLD Using Ordered Statistics for Low Rate Codes 772

Ryuhei Yokoyama, Takuya Kusaka, Toru Fujiwara

LS2-We-1 : Cryptography VI

Update on *Enocoro* Stream Cipher 778

Dai Watanabe, Toru Owada, Kazuto Okamoto, Yasutaka Igarashi, Toshinobu Kaneko

On the truncated path search for the maximum differential characteristic probability on a generalized Feistel-type block cipher 784

Yasutaka Igarashi, Toshinobu Kaneko

A Security Evaluation of Certain Stream Ciphers which Involve Randomness and Coding 789

Miodrag Mihaljević, Hideki Imai

A Structured Aggregate Signature Scheme 795

Naoto Yanai, Eikoh Chida, Masahiro Mambo

CW-We-1 : Shannon Theory II

A Revisit to The Muroga Method of Computing Channel Capacity 801

Tsutomu Kawabata

Block Fading Channels with Limited Channel State Information 807

S. Lembo, C.-H. Yu, O. Tirkkonen

The Achievable Rate of Stationary Rayleigh Flat-Fading Channels with IID Input Symbols 812
Meik Dörpinghaus, Heinrich Meyr, Gerd Ascheid

The Capacity Region of a Class of Relay-Broadcast Channels and Relay Channels with Three Parallel Unmatched Subchannels 818
Reza Khosravi-Farsani, Bahareh Akhbari, Mohammad Reza Aref

Au-We-1 : Sequences

Suitable Representation of Values on the Logistic Map with Finite Precision 824
Shunsuke Araki, Ken'ichi Kakizaki, Takeru Miyazaki, Satoshi Uehara

A Study on Differences in Properties of the Logistic Maps over Integers Affected by Rounding 830
Takeru Miyazaki, Shunsuke Araki, Satoshi Uehara

Autocorrelation Functions and Double Difference Sequences 836
Ying Li, Yi-Chan Kao, Mei-Wen Chang

Hamming Distance Correlation for q -Ary Constant Weight Codes 842
Takayasu Kaida, Junru Zheng

ES1-We-2 : Error-Control Coding III

An Algorithm for New Lower Bound of Minimum Distance by DFT for Cyclic Codes 846
Junru Zheng, Takayasu Kaida

Maximum a Posteriori Estimation Using ARCH Models and Burst Error Correcting Array Codes for Burst-Erasure Recording Channels 850
Hidetoshi Saito, Ryuji Kohno

Comparison of Reed-Solomon and Raptor codes for the protection of Video On-Demand on the erasure channel 856
Julie Neckebroek, Marc Moeneclaey, Enrico Magli

Analysis of Quasi-Cyclic LDPC codes under ML decoding over the erasure channel 861
Mathieu Cunche, Valentin Savin, Vincent Roca

Floating Codes with Good Average Performance 867
Hiroshi Kamabe

ES2-We-2 : MIMO III

Informed Message Update for Iterative MIMO Demapping and Turbo Decoding 873
Dan Zhang, I-Wei Lai, Konstantinos Nikitopoulos, Gerd Ascheid

Imperfect Generalized Transmit Beamforming With Co-channel Interference Cancelation 879
Redha M. Radaydeh, Mohamed-Slim Alouini

Distributed Precoding Design for MIMO Interference Channels 885
Ronghong Mo , Yong Huat Chew, Tony Q. S. Quek, Chengzhi Chen

Analysis of Diversity-Multiplexing Tradeoff Bounds of ZF-SIC Systems with Error Propagation 890
Dong-Min Shin, Kyeongcheol Yang

Digital-Controlled Analog Beamforming for Indoor MIMO Multipath Channels 895
Yabo Li

LS2-We-2 : Cryptography VII

Two-Sided Multiplications are Reduced to One-Sided Multiplication in Linear Piece In Hand Matrix Methods 900
Kohtaro Tadaki, Shigeo Tsujii

Clarifying the Specification of Linear Piece In Hand Matrix Method 905
Kohtaro Tadaki, Shigeo Tsujii

A Generic Weakness of the k -normal Boolean Functions Exposed to Dedicated Algebraic Attack 911
Miodrag Mihaljević, Sugata Gangopadhyay, Goutam Paul, Hideki Imai

On the security of the quantum key distribution using the Mean King Problem 917
Masakazu YOSHIDA, Takayuki MIYADERA, Hideki IMAI

Information Reconciliation for QKD with Rate-Compatible Non-Binary LDPC Codes 922
Kenta KASAI , Ryutaroh MATSUMOTO, Kohichi SAKANIWA

CW-We-2 : Cognitive and Software Radio

Design and Implementation of Low Power Digital Phase –Locked Loop 928
M. Saber, Y. Jitsumatsu, M. T. A. Khan

Downlink Beamforming Optimization for Cognitive Underlay Networks 934
Youngmin Jeong, Tony Q. S. Quek, Hyundong Shin

Analysis of Primary User Duty Cycle Impact on Spectrum Sensing Performance 940
Kevin Chang, Yu Chieh Huang, Bouchra Senadji

Optimal Multiuser Beamforming and Power Allocation for Hierarchical Cognitive Radio Systems 946
Meng-Lin Ku, Li-Chun Wang, Yu Ted Su

Cognitive Interference Channel with Two Confidential Messages 952
Hamid G. Bafghi, Somayeh Salimi, Babak Seyfe, Mohammad R. Aref

Au-We-2 : Cooperative Communications II

Relay-Aided Multi-Cell Broadcasting with Random Network Coding 957
Lu Lu, Fan Sun, Ming Xiao, Lars K. Rasmussen

Subcarrier Allocation and Partner Selection Algorithms for Cooperative Multicarrier Systems 963
Kuang-Yu Sung, Y.-W. Peter Hong, Chi-chao Chao

Outage Performance Analysis for Fractional Frequency Reused TDD-OFDMA Systems with Asymmetric 969
Traffics
Li-Chun Wang, Wei-Chi Li

Outage Analysis and Optimal Power allocation for Network-coding-based Hybrid AF and DF 975
Jooha Bek, Jaeyoung Lee, Jun Heo

Cooperative MMSE OFDM Receiver for Half-Duplex and Multiple-Relays System 981
Rih-Lung Chung, Shu-Hao Chang

ES1-We-3 : RS/AG Codes

Decoding Reed-Solomon Codes up to the Sudan Radius with the Euclidean Algorithm 986
Alexander Zeh, Wenhui Li

Syndrome Calculation for the Decoding of Algebraic-Geometry Codes on Plane Garcia-Stichtenoth Curves 991
Chung-Chin Lu, Chih-Yen Yang, Ti-Chung Lee

A New Reliability Updating Scheme for Iterative Decoding of Reed-Solomon Codes with Refined 995
Initialization
Jian-Jia Weng, Yu-Min Hsieh, Hsin-Chuan Kuo, Chung-Hsuan Wang, Tsung-Cheng Wu, Yi-Sheng Su

Unified system of encoding and decoding erasures and errors for algebraic geometry codes 1001
Hajime Matsui

ES2-We-3 : Multiuser Information Theory III

Outage Capacity of Bursty Amplify-and-Forward with Incremental Relaying 1007
T. Renk, H. Jäkel, F. K. Jondral, D. Gündüz, A. Goldsmith

Non-Coherent Two-Way Relaying: Rate Bounds for the high SNR Regime 1012
Zoran Utkovski, Aydin Sezgin, Juergen Lindner

Achievable Rate Regions for Interference Channel with Two Relays 1018
Bahareh Akhbari, Mahtab Mirmohseni, Mohammad Reza Aref

Generalized Multiple-Access Relay Channel with Confidential Messages 1024
Amir Sonee, Somayeh Salimi, Mahmoud Salmasizadeh

LS2-We-3 : Quantum Information

Generalized Wigner-Yanase-Dyson Skew Information and Uncertainty Relation 1030
Kenjiro Yanagi

Formula of channel matrix for coded quantum signals by classical linear codes over Z_m 1035
Masaki Ota, Hideyuki Kumazawa, Keisuke Shiromoto, Tsuyoshi Sasaki Usuda

A Further Study on the Encoding Complexity of Quantum Stabilizer Codes 1041
Kao-Yueh Kuo, Chung-Chin Lu

On attainment of the capacity of broadband quantum channel by wavelength division multiplexing 1045
Yoshio Takamura, Shogo Usami, Tsuyoshi Sasaki Usuda

CW-We-3 : OFDM PAPR

A Modified Genetic Algorithm PTS Technique with Error Correction for PAPR Reduction in OFDM Systems 1050
Hsinying Liang, Zhe Lin, Houshou Chen, Cheng-Ying Yang

A New Selected Mapping Scheme for PAPR Reduction in OFDM Systems 1054
Kee-Hoon Kim, Hyun-Bae Jeon, Jong-Seon No, Dong-Joon Shin

PAPR for OFDM and the Proportion of Information Bearing Signals for Tone Reservation 1058
Holger Boche, Brendan Farrell