2008 International Symposium on Information Theory and its Applications

(ISITA)

Auckland, New Zealand
7 – 10 December 2008

Pages 1-536
# TABLE OF CONTENTS

## COOPERATIVE COMMUNICATION

**A Study on Cooperative Reception of One Segment ISDB-T**

Takashi Okubo, Makoto Itami

**Multilevel Coded Cooperation: Concepts and Design Criteria**

Koji Ishii, Koji Ishibashi, Hideki Ochiai

**Collaborative Communications using Bit-Interleaved Coded DPSK with Cyclic Delay Diversity**

Yuta Nakao, Koji Ishibashi, Ryuji Kohno

**Collaborative Diversity Enhancements using Rate-Compatible Turbo Codes**

Koji Ishibashi, Koji Ishii, Hideki Ochiai

## SECRET SHARING

**A Construction of a Visual Secret Sharing Scheme for Plural Secret Images and its Basic Properties**

Hiroki Koga, Masayuki Miyata

**On Some Properties of the (t, n) Threshold Secret Sharing Schemes Based on the Generalized Vector Space Construction**

Todorka Alexandrova, Hiroyoshi Morita

**A Construction Method of Secret Sharing Schemes Based on Authorized Subsets**

Kouya Tochikubo

**Weakly Secure Visual Secret Sharing Schemes**

Mitsugu Iwamoto

## WIRELESS NETWORKS 1

**Performance Evaluation of Effect of Nonlinear Distortion in SC-FDMA System**

Shinya Suzuki, Osamu Takyu, Yohtaro Umeda

**A Study on Energy-Efficient Protocol Based on the CSMA/CA in Ad-Hoc Networks**

Hiroyasu Masuno, Kensaku Asahi, Akira Watanabe, Akira Ogawa

**A Cluster Relay Coded Cooperative Strategy in Broadband Wireless Ad-Hoc Networks**

Shinsuke Ibi, Setichi Sampei

**Clustering and Labeling of Orthogonal Signals for Modulation Identification**

Takahiro Yamamoto, Ikuo Oka, Shingo Ata

## LDPC CODES 1

**Rate Estimation Scheme for Weighted Bit-Flipping Decoding of Rate Compatible LDPC Codes**

Kenji Kita, Tetsuo Tsujioka

**Towards Universal Cover Decoding**

Nathan Axvig, Deanna Dreher, Katherine Morrison, Eric Psota, Lance C. Pérez, Judy L. Walker
Gradient Descent Bit Flipping Algorithms for Decoding LDPC Codes .......................................................... 81
  Tadashi Wadayama, Keisuke Nakamura, Masayuki Yagita, Yuuki Funahashi, Shogo Usami, Ichi Takumi

LLR Metrics for LDPC Codes with Quadrature Differential PSK Transmission and their Performances .......................................................... 87
  Elisa Mo, Pooi Yuen Kam, Marc A. Armand

STORAGE SYSTEMS

On the Capacity of Flash Memories .................................................................................................................. 93
  Anxiao Andrew Jiang, Jehoshua Bruck

Burst Detection by Parity Check Matrix of LDPC Code for Perpendicular Magnetic Recording Using Bit-Patterned Medium .......................................................................................... 99
  Yasuaki Nakamura, Yoshihiro Okamoto, Hisashi Osawa, Hiroaki Murakami, Hajime Aoi

Rewritable Storage Channels .......................................................................................................................... 105
  L.A. Lastras-Montano, M. Franceschini, T. Mittelholzer, M. Sharma

A Reliable Soft-Output of Autoregressive ML Detector for Perpendicular Magnetic Recording with Intertrack Interference .................................................................................................. 111
  Kohsuke Harada, Hironori Uchikawa

SOURCE AND CHANNEL CODING

The Overall Performance of the Shannon Code ................................................................................................ 117
  Mohammadali Khosravifard, M. Razaviyayn, H. Narimani, T. Aaron Gulliver

Random Coding Bounds for Correlated Parallel Channels with Unidirectionally Cooperating Decoders .......................................................................................................................... 121
  Hideki Yagi, Manabu Kobayashi, Shigeichi Hirasawa

On the Capability of the Harada-Kobayashi Algorithm in Finding Fix-Free Codewords .................................. 127
  Mohammadali Khosravifard, T. Aaron Gulliver

A Distributed Source Coding Framework for Multiple Sources ........................................................................ 131
  Xiaomin Cao, Margreta Kuijper

OPTICAL COMMUNICATION AND BROADCASTING SYSTEMS

Effect of One-Way Mode of Hybrid Reservation on Slotted Optical Burst Switching Networks .................................................. 135
  Hiroyuki Noguchi, Koji Kamakura

Outage Probability of the Free-Space Optical Channel with Doubly Stochastic Scintillation ................................ 141
  Nick Letzepis, Albert Guillén i Fàbregas

Increased Throughput using Optical PPM-CDMA .............................................................................................. 147
  Yusuke Kozawa, Hiromasa Habuchi

Hierarchical Modulation in DVB-T/H Mobile TV Transmission over Fading Channels .................................. 153
  Tomas Kratochvil, Radim Stukavec

OFDM 1

Effect of Ranging Error on Base Station Cooperation OFDM System .............................................................. 159
  Minjoo Kim, Osamu Miyagi, Ian Dexter Garcia, Kei Sakaguchi, Kiyomichi Araki
Resource Allocation for the Downlink of OFDMA Cellular Networks and Optimization of the Reuse Factor
Nassar Ksairi, Pascal Bianchi, Philippe Ciblat, Walid Hachem

Level Crossing Analysis of BER for Adaptive MIMO OFDM Systems
Krishna P. Kongara, Peter J. Smith

Effect of Channel Mismatch on AMC in Asymmetric TDD/OFDM System with Pre-Equalization in Downlink
Nandar Lynn, Koichi Adachi, Osamu Takyu, Masao Nakagawa

BROADCAST ENCRYPTION

Group Key Rekeying Using the LKH Technique and the Huffman Algorithm
Takahito Sakamoto, Takashi Tsuji, Yuichi Kaji

A Practical Key Management Scheme using the Frame-Based Features for Layered Access Control of H.264/SVC
Su-Wan Park, Dohee Yi, Sang-Uk Shin

Hierarchical Encryption of Motion JPEG2000 Codestreams for Layered Multicast Transmission
Takayuki Nakachi, Kan Toyoshima, Yoshihide Tomomura, Tatsuya Fujii

Criteria of Aptitude of a Key-Management Tree for a Frequency Distribution of Communication
Nozomu Ochiumi, Fumiaki Kanazawa, Masahiro Yanagida, Eiji Okamoto, Yasuichi Horibe

WIRELESS NETWORKS 2

A Lower Bound to Transmission Power for Multicast in Underwater Networks using Network Coding
Daniel E. Lucani, Muriel Médard, Milica Stojanovic

A Novel Ad-Hoc Network Routing Protocol with an Acceleration Sensor
Wataru Uemura, Yukihiro Kuga, Masashi Murata

A New Framework for Opportunistic Scheduling in Wireless Networks
Jang-Won Lee, Jeong-Ahn Kwon

A Proposal of Gateway Decentralization Method in Wireless Mesh Networks and its Evaluation
Masashi Ito, Toshihiro Shikama, Akira Watanabe

LDPC CODES 2

A Class of Invertible Circulant Matrices for QC-LDPC Codes
Marco Baldi, Federico Bambozzi, Franco Chiaraluce

Efficient Encoding of QC-LDPC Codes Related to Cyclic MDS Codes
Norifumi Kamiya, Eisaku Sasaki

Improvement of the Davey-MacKay Construction
Johann A. Briffa, Hans Georg Schaathun

Determination of the Shortest Balanced Cycles
Yuansheng Tang, Xinmei Huang, Jinli Wang, Ming Chen
SHANNON THEORETIC SECURITY

Secret Communication with Feedback ................................................................. 244
Deniz Gunduz, D. Richard Brown, H. Vincent Poor

New Coding Theorems for Fixed-Length Source Coding and Shannon's Cipher System
with a General Source ..................................................................................... 250
Hiroki Koga

MIMO Broadcasting with Common, Private and Confidential Messages ............. 256
Hung D. Ly, Tie Liu, Yingbin Liang

An Information-Theoretic Cryptanalysis of Network Coding - Is Protecting the Code
Enough? ........................................................................................................ 262
Luisa Lima, João Vilela, João Barros, Muriel Medard

ESTIMATION

Entropy Estimation using MDL and Piecewise Constant Density Models ............. 268
Gilles Menez, Maria-João Rendas, Eric Thierry

On Estimation in Networked Control Systems with Random Delays and Partial
Observation Losses ..................................................................................... 274
Matteo Trivellato, Nevio Benvenuto

On Recurrence Formulas for Computing the Stochastic Complexity .................. 280
Tommi Mononen, Petri Myllymäki

Exact Optimality of the Shiryaev-Roberts Procedure for Detecting Changes in
Distributions ............................................................................................... 286
Moshe Pollak, Alexander G. Tartakovsky

QUANTUM INFORMATION THEORY 1

Efficient Quotient Codes Decodable in Polynomial Time for Quantum Error Correction
and Cryptography ..................................................................................... 292
Mitsuru Hamada

The Algebraic Structure of Mutually Unbiased Bases ....................................... 298
Joanne L. Hall, Asha Rao

Quantum Secret Sharing between Multiparty and Multiparty against the Attacks with
Single Photons or EPR-Pair ......................................................................... 303
Atsushi Waseda, Takayuki Takagi, Masakazu Soshi, Atsuko Miyaji

OFDM 2

A Low-Complexity Selective Mapping PAPR Reduction Scheme for Coded MIMO-OFDM ................. 307
Yung-Chih Tsai, Tien-Hui Chen, Yu-Hung Lo, Mao-Chao Lin

New SLM Scheme for PAPR Reduction in OFDM Signals ................................ 311
Kyu-Hong Kim, Hyun-Bae Jeon, Jong-Seon No, Dong-Joon Shin

Efficient Optimization for Tone Reservation OFDM ........................................ 315
Abolfazli Ghassemi, T. Aaron Gulliver

On the Performance of Clipping Noise Cancellation for OFDM Systems with High-Order
Coded Modulation .................................................................................... 321
Toru Uchino, Hideki Ochiai
Adaptive TR Scheme for OFDM Signals ................................................................. 326
Dae-Woon Lim, Hyung-Suk Noh, Hyun-Bae Jeon, Jong-Seon No, Dong-Joon Shin

**ID-BASED ENCRYPTION**

Efficient ID-Based Key Agreement Protocol under the DLDH Assumption without Random Oracles ................................................................. 330
Daisuke Moriyama, Hiroshi Doi

A Forward Secure Identity Based Encryption Scheme with Master Key Update ................................................................. 336
Peng Yang, Kanta Matsuura

Flexible Identity Based Attribute Encryption from Identity Based Broadcast Encryption ................................................................. 342
Ryuichi Sakai

Stateful Public Key Encryption: How to Remove Gap Assumptions and Maintaining Tight Reductions ................................................................. 346
Peng Yang, Rui Zhang, Kanta Matsuura

On Security Enhancement of Long-Term Private Key for the Tripartite Authenticated Key Agreement Protocol ................................................................. 352
Masahiro Nomura, Katsuhiro Nakamura

**DETECTION AND ESTIMATION**

Asymptotic Performance Bounds of Joint Channel Estimation and Multiuser Detection in Frequency-Selective Fading DS-CDMA Channels ................................................................. 358
Keigo Takeuchi, Mikko Vehkaperae, Toshiyuki Tanaka, Ralf R. Mueller

A New Transform for Chirp Detection ................................................................. 364
Xiumei Li, Guoan Bi

Iterative Delay Compensation Algorithm to Mitigate NLOS Influence for Positioning ................................................................. 369
Koji Enda, Ryuji Kohno

Bayesian Probability of Error under Fine Quantization ................................................................. 375
Soumya Jana

A Random Sets Framework for Error Analysis in Estimating Geometric Transformations --A First Order Analysis ................................................................. 381
Rami Hagege, Joseph M. Francos

**ALGEBRAIC CODES**

The Error Locator Polynomial for Correctable (t+1)-Error of RS Codes ................................................................. 385
Masami Mohri, Masakatu Morii

On Extremal Binary Doubly-Even Self-Dual Codes of Length 88 ................................................................. 391
Radinka Yorgova, Nuray At

A Constructing Approach of the Roos Bound for Cyclic Codes ................................................................. 394
Takayasu Kaida, Junru Zheng

Unified Systems of Encoding and Decoding for a Class of Algebraic-Geometric Codes ................................................................. 400
Hajime Matsui

**DATA NETWORKS 1**

Online Network Coding for Optimal Throughput and Delay - the Three-Receiver Case ................................................................. 406
Jay Kumar Sundararajan, Devavrat Shah, Muriel Medard
Path Diversity Effects of Binary Tree Network Composed of Binary Symmetric Channels
Shinji Tani, Ikuo Oka, Shingo Ata

A Shared-Relay Cooperative Diversity Scheme Based on Joint Channel and Network Coding
Xiaoyan Xu, Mark F. Flanagan, Christian Koller, Norbert Goertz

Multi-Bit Revocable Network Coding Scheme for Butterfly-Like Network
Hidenori Kuwakado, Masakatu Morii

QoS Network Coding
Amir Hesam Salavati, Babak Hossein Khalaj, Pedro M. Crespo, Mohammad Reza Aref

PATTERN RECOGNITION AND LEARNING

Multi-Class Support Vector Machine for Human Posture Classification using a Simplified Shock Graph
Shahrani Shahbudin, Aini Hussain, Nooritawati Md. Tahir, Salina Abdul Samad

Asymptotic Evaluation of Distance Measure on High Dimensional Vector Spaces in Text Mining
Masayuki Goto, Takashi Ishida, Makoto Suzuki, Shigeichi Hirasawa

Weed Detection System using Support Vector Machine
Asnor Juraiza Ishak, Mohd Marzuki Mustafa, Noritawati Md Tahir, Aini Hussain

Refinement of Index Term Set and Improvement of Classification Accuracy on Text Categorization
Makoto Suzuki, Takashi Ishida, Masayuki Goto

QUANTUM INFORMATION THEORY 2

Generalized Wigner-Yanase Skew Information and Generalized Fisher Information
Kenjiro Yanagi, Shigeru Furuichi, Ken Kuriyama

A Simple and Efficient Solution of the Identifiability Problem for Hidden Markov Sources and Quantum Random Walks
Alexander Schoenhuth

Separability Criterion in Prime Dimensions based on Landau-Pollak Uncertainty Relation
Masakazu Yoshida, Takayuki Miyadera, Hideki Imai

The Multiple Coding Gain with Two Criteria in an Attenuated Quantum Channel
Ryosuke Sahara, Shogo Usami, Tsuyoshi Usuda

COMMUNICATION SYSTEMS 1

Outage Probability for MMSE Linear Diversity in a Non-Gaussian Fading Environment
Narongrit Mekloi

Outage Performance of a Novel Relaying Protocol: Decode or Quantize and Forward
Pascal Bianchi, Philippe Ciblat, Walid Hachem

On the Achievable Rate of Stationary Rayleigh Flat-Fading Channels with Gaussian Input Distribution
Meik Dörpinghaus, Martin Senst, Gerd Ascheid, Heinrich Meyr

Expectations of a Noncentral Chi-Square Distribution with Application to IID MIMO Gaussian Fading
Stefan M. Moser
Effect of Doppler Shift on Performance of Binary DPSK over Fast Rician Fading Channels with Diversity Reception

Hua Fu, Pooi Yuen Kam

KEY EXCHANGE

Security Verification for Authentication and Key Exchange Protocols

Haruki Ota, Shinsaku Kiyomoto, Toshiaki Tanaka

A Study on a Key Establishment Scheme with QC LDPC Codes and UH-Protocols

Yuto Matsunaga, Manabu Hagiwara, Kazukuni Kobara, Hideki Imai

Deniable Ring Authenticated Private Key Establishment

Elliot T. Taniguchi, Hirosuke Yamamoto

A Group-Key Agreement Protocol Secure against the Malleability Attacks

Seiko Arita, Akihiko Sakuma

A Ramp Scheme for Key Predistribution System against Collusion of Users and Centers

Takahiro Yoshida, Toshiyasu Matsushima, Hideki Imai

SPREAD SPECTRUM 1

Performance Analysis of Multi-Antenna Pre/Post-Rake Transmission for UWB-IR System under Channel Estimation

Jun Hioki, Makoto Itami

Error Probability in Presence of Detection Timing Error for ISI-Free Roll-Off Tunable Pulse

Masayuki Mohri, Masanori Hamamura

Performance Analysis of Signal Detection using Quantized Received Signals of Linear Vector Channel

Kazutaka Nakamura, Toshiyuki Tanaka

Performance Evaluation of CSK Spread Spectrum Boomerang System

Toru Sugimoto, Tsuyoshi Arai, Hiroshi Inai

Throughput Evaluation of the Nonorthogonal CSK/CDMA ALOHA with Interference C canceler

Nobuyoshi Komuro, Hiromasa Habuchi, Toshinori Tsuboi

CODED MODULATION

Double Error Correctable Integer Code and its Application to QAM

Hristo Kostadinov, Hiroyoshi Morita, Noburo Iijima, Nikolai Manev

Noncoherent Iterative Decoding of Symbol Insertion Systems

Makoto Tanahashi, Hideki Ochiai

Modulation Codes for Reader-Tag Communication on Inductively Coupled Channels

Angela I. Barbero, Greg D. Horler, Eirik Rosnes, Øyvind Ytrehus

Investigation on the Chaotic Phase Shift Keying (CPSK) System with Turbo Iterative Coding

Xin Wu, Stevan Berber
LOSSY SOURCE CODING

Application of LCLP to Lossy Source Coding ................................................................. 589
Shigeki Miyake, Junya Honda, Hirosuke Yamamoto

Typical Performance of Irregular LDGM Codes for Lossy Compression ....................... 595
Kazushi Mimura

On Logarithmic Spherical Vector Quantization ............................................................... 600
Hauke Krueger, Raimund Schreiber, Bernd Geiser, Peter Vary

Lossy Source Coding Algorithm using Lossless Multi-Terminal Source Codes ............... 606
Jun Muramatsu, Shigeki Miyake

STOCHASTIC AND SIGNAL PROCESSING

Development of a Direction Indicating System for a Tele-Support for the Visually
Impaired............................................................................................................................ 612
Takafumi Ienaga, Yu Yoneda, Chikamune Wada, Yoshihiko Kimuro, Michito Matsumoto

A Study of Region Extraction and System Model on an Observation System of Time-
Sequenced 3-D CT Images ............................................................................................. 618
Yoshio Yanagihara

Determining an Appropriate Range of Image Resolutions for Appearance-Based Object
Detection and Haar-Like Feature Extraction .................................................................. 623
Anselm Haselhoff, Anton Kummert

Improving Face Recognition using Original and Pre-Processed Features ....................... 628
Nor’aini Abdul Jalil, P. Raveendran

BOUNDS ON ERROR PROBABILITY

Bounds on Error Probability of Block Codes with Bounded-Angle Maximum-Likelihood
Incomplete Decoding ...................................................................................................... 634
Sam Dolinar, Kenneth Andrews, Fabrizio Pollara, Dariush Divsalar

Kovalenko’s Full-Rank Limit and Overheads as Lower Bounds of Error-Performances of
LDPC and LT Codes over Binary Erasure Channels ...................................................... 640
Ki-Moon Lee, Hayder Radha, Beom-Jin Kim, Hong-Yeop Song

Fast Simulation Method of BER Performance of Error Correcting Codes over AWGN
Channel ............................................................................................................................ 645
Haruo Ogiwara, Yasunori Hori, Toshiyuki Shohon

Tight BER Bounds of Binned Orthogonal and Quasi-Orthogonal Dirty-Paper Codes .......... 650
Xiaotian Xu, Yong Liang Guan

MIMO 1

A Robust Cooperative Relaying Strategy for Wireless Networks using Semidefinite
Constraints and Worst-Case Performance Optimization ................................................. 655
Ranaji Krishna, Kanapathippillai Cumanan, Vimal Sharma, Sangarapillai Lambotharan

High and Low-SNR Regimes for Stochastic Networks ..................................................... 660
Giussi Alfano, Maxime Guillaud, Antonia Tulino

MIMO Relay Design for Multiple Link Pairs based on SINR Constraints .......................... 666
Jiun-Je Jian, Hsuan-Jung Su, Hsueh-Jyh Li
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Stream Multiplexing for MIMO Two-Way Mesh Networks</td>
<td>672</td>
</tr>
<tr>
<td>Fumie Ono, Kei Sakaguchi, Takayuki Sugiyasu</td>
<td></td>
</tr>
<tr>
<td>Two-Hop Transmission with Second-Hop Channel State Information</td>
<td>678</td>
</tr>
<tr>
<td>Majid N. Khormuji, Mikael Skoglund</td>
<td></td>
</tr>
<tr>
<td><strong>FINGERPRINT AND STENOGRAPHY</strong></td>
<td></td>
</tr>
<tr>
<td>Hierarchical Construction of Tardos Code</td>
<td>683</td>
</tr>
<tr>
<td>Naoyuki Akashi, Minoru Kuribayashi, Masakatu Morii</td>
<td></td>
</tr>
<tr>
<td>Detection of BPCS-Steganography Using SMWCF Steganalysis and SVM</td>
<td>689</td>
</tr>
<tr>
<td>Julio Lopez-Hernandez, Raul Martinez-Noriega, Mariko Nakano-Miyatake, Kazuhiro Yamaguchi</td>
<td></td>
</tr>
<tr>
<td>Effective Assignment of Fingerprints on CDMA-Based Fingerprinting Scheme</td>
<td>694</td>
</tr>
<tr>
<td>Hiroshi Kato, Minoru Kuribayashi, Masakatu Morii</td>
<td></td>
</tr>
<tr>
<td>Regaining Synchronization using Neural Networks to Detect Watermark Codes</td>
<td>700</td>
</tr>
<tr>
<td>Reolyn Heymann, Hendrik C. Ferreira</td>
<td></td>
</tr>
<tr>
<td>A Group Testing Based Deterministic Tracing Algorithm for a Short Random Fingerprint Code</td>
<td>706</td>
</tr>
<tr>
<td>Takashi Kitagawa, Manabu Hagiwara, Koji Nuida, Hajime Watanabe, Hideki Imai</td>
<td></td>
</tr>
<tr>
<td><strong>SPREAD SPECTRUM 2</strong></td>
<td></td>
</tr>
<tr>
<td>Development of a Reverse Chaos Based CDMA Link and Fading Mitigation</td>
<td>711</td>
</tr>
<tr>
<td>Xinghua Zhan, Stevan Berber</td>
<td></td>
</tr>
<tr>
<td>Performance of the Slot-Distributed Push-Type Packet Compensation Protocol for the Road to Vehicle Broadcasting System</td>
<td>717</td>
</tr>
<tr>
<td>Koichiro Hashitohara, Hiromasa Habuchi</td>
<td></td>
</tr>
<tr>
<td>Suppression of Partial-Band-Noise Jamming for FFH/MFSK Systems over Frequency-Selective Rician-Fading Channels</td>
<td>722</td>
</tr>
<tr>
<td>Jiliang Zhang, Kah Chan Teh, Kwok Hung Li</td>
<td></td>
</tr>
<tr>
<td>Improving Ranging Accuracy by Two-Step TOA Estimation for UWB Radio</td>
<td>726</td>
</tr>
<tr>
<td>Chizu Fukao, Masaya Sasaki, Kohei Ohno, Makoto Iiomi</td>
<td></td>
</tr>
<tr>
<td><strong>LDPC CODES 3</strong></td>
<td></td>
</tr>
<tr>
<td>Three-Edge type LDPC Code Ensembles with Exponentially Few Codewords with Linear Small Weight</td>
<td>731</td>
</tr>
<tr>
<td>Tomoharu Awano, Kenta Kasai, Tomoharu Shibuya, Kohichi Sakaniwa</td>
<td></td>
</tr>
<tr>
<td>The Vertex-Cut Bound and its Applications</td>
<td>737</td>
</tr>
<tr>
<td>Navin Kashyap</td>
<td></td>
</tr>
<tr>
<td>Computation of Zeta Functions Counting Pseudo-Codewords of Linear Codes</td>
<td>743</td>
</tr>
<tr>
<td>Shozo Matsuda, Seiken Saito, Toyokazu Hiramatsu</td>
<td></td>
</tr>
<tr>
<td>Weight Distribution of Non-Binary LDPC Codes</td>
<td>748</td>
</tr>
<tr>
<td>Kenta Kasai, Charly Poulliat, David Declercq, Tomoharu Shibuya, Kohichi Sakaniwa</td>
<td></td>
</tr>
<tr>
<td>Approximate Examination of Trapping Sets of LDPC Codes Using the Probabilistic Algorithm</td>
<td>754</td>
</tr>
<tr>
<td>Masanori Hirotomo, Yoshiho Konishi, Masakatu Morii</td>
<td></td>
</tr>
</tbody>
</table>
DATA NETWORKS 2

Multicast Capacity of Multiple Access Erasure Networks .......................................................... 760
Kiran T. Gowda, Sun Sumei

Information Interflow Network (I2N) using LDPC Codes ........................................................ 766
Yugo Haruta, Koji Ishibashi, Tadahiro Wada

Capacity of Broadcast Erasure Networks Using Spatial Network Coding .................................. 772
Mehrdad Salmasi, S. Jamaloddin Golestani

Maximum Multicommodity Flow of Small-World Networks ...................................................... 778
Je-Wei Chang, Chien Chen, Rong-Hong Jan

SIGNAL PROCESSING 1

On the Stability of a Generalized Shannon Sampling Theorem .................................................. 784
Yufang Hao, Achim Kempf

On the Singularity of Laplace-Stieltjes Transform of a Heavy Tailed Random Variable ........ 790
Kenji Nakagawa

On the Minimum Sampling Rate of Signals of Non-bandlimited Response ........................... 794
Beilei Huang, Edmund M-K. Lai

On Relationship between Loss Probability and Utilization Factor on Real-Time Basis .......... 800
Mikihiko Nishiara

MULTI-TERMINAL INFORMATION THEORY 1

Gaussian Z-Interference Channel with a Relay Link: Achievable Rate Region and
Asymptotic Sum Capacity .................................................................................................................. 805
Lei Zhou, Wei Yu

Capacity Region of Quasi-Asynchronous Discrete Multiple-Access Channel .......................... 811
Yoichiro Watanabe, Jun Cheng, Koichi Kamoi

On Broadcast with a Common Message over Networks ............................................................. 817
Dinkar Vasudevan, Satish Babu Korada

A New Graph Perspective on Max-Min Fairness in Gaussian Parallel Channels .................... 823
Marcin Wiczanowski, Holger Boche

Optimal Time-Division of Two-Phase Decode-and-Forward Bidirectional Relaying ............ 829
Tobias J. Oechtering, Rafael F. Wyrembelski, Holger Boche

MIMO 2

On the Ergodic Performance of a Simple Closed-Loop Spatial Multiplexing Architecture ........ 835
Thomas Hunziker, Thomas Edlich, Dirk Dahlhaus

Asymptotic Mutual Information of Multiple-Path Rician Fading MIMO Multiple-Access
Channel ........................................................................................................................................... 841
Chao-Kai Wen, Jung-Chieh Chen, Kai-Kit Wong, Pangan Tin

Improving Capacity in MIMO Systems with Asynchronous PAM ........................................... 847
Kishor Barman, Onkar Dabeer

Capacity Analysis for MIMO Two-Hop Two-Relay Amplify-and-Forward Relaying
Systems ............................................................................................................................................ 853
Abdulla Firag, Peter J. Smith
WATERMARKING

Multichannel Audio Watermarking Method by Multiple Embedding .............................................. Harumi Murata, Akio Ogihara, Motoi Iwata, Akira Shiozaki

A DWT-Based Video Watermarking Scheme Resilient to MPEG-2 Compression and Collusion Attacks ............................................................... Raul Martínez-Noriega, Rogelio Reyes, Clara Cruz, Mariko Nakano-Miyatake, Héctor Pérez

Adaptive Reversible Data Hiding for JPEG Images .................................................................................. Hirofumi Sakai, Minoru Kuribayashi, Masakatu Morii

Evaluation of Noticeable Areas Using the Difference in Power of Frequency Domain for Digital Watermarking ......................................................... Motoi Iwata, Akira Shiozaki

SPREAD SPECTRUM 3

A Set of Binary Sequences Obtained from 4 Preferred M-Sequences .................................................. Daisuke Masuda, Tsutomu Moriuchi, Satoshi Uehara

Basic Properties of the Complete Complementary Codes Using the DFT Matrices and the Kronecker Products ............................................................ Yi Jin, Hiroki Koga

On the Parameters for CT-CDMA Communication Systems Based on Complete Complementary Codes ........................................................................... Tetsuya Kojima, Masahiro Aono

A Model of WCDMA Radio Interface with Reservation ........................................................................ Maciej Stasiak, Slawomir Hanczewski

LDPC CODES 4

Variable-to-Check Residual Belief Propagation for Informed Dynamic Scheduling of LDPC Codes ........................................................................................................... Jung-Hyun Kim, Mi-Young Nam, Hong-Yeop Song, Ki-Moon Lee

Improvement of the Forced-Convergence Decoding for LDPC Codes .................................................. Rumi Aoyama, Yuichi Kaji

Modified Min-Sum Algorithm with Threshold Filtering for Nonbinary LDPC Codes over GF(q) ........................................................................................................... Yue Liu, Jun Ning, Jinhong Yuan

New Stopping Criteria for Decoding LDPC Codes in H-ARQ Systems ................................................ Beomkyu Shin, Sang-Hyo Kim, Jong-Seon No, Dong-Joon Shin

SENSOR NETWORKS

Power Efficient State Estimation Using Multiple Sensors ........................................................................ Alex S. Leong, Subhrakanti Dey, Jamie S. Evans

Joint Channel Decoding of Spatially and Temporally Correlated Data in Wireless Sensor Networks ........................................................................................................... Kentaro Kobayashi, Takaya Yamazato, Hiraku Okada, Masaaki Katayama

Random Distributed Detection for Wireless Sensor Networks .......................................................... Xiao Liang, Wei Li, T. Aaron Gulliver
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BER Performance of Turbo Coded Multi-Hop Networks using Iterative Channel Information Estimation Scheme</td>
<td>939</td>
</tr>
<tr>
<td>Kouji Ohuchi, Tadahiro Wada, Hiraku Okada, Masato Saito</td>
<td></td>
</tr>
<tr>
<td><strong>SIGNAL PROCESSING 2</strong></td>
<td></td>
</tr>
<tr>
<td>Positioning and Tracking Algorithm Using Node Selection Method in Wireless Sensor Networks</td>
<td>944</td>
</tr>
<tr>
<td>Yutaka Kashiwabara, Kentaro Taniguchi, Ryuji Kohno</td>
<td></td>
</tr>
<tr>
<td>UWB-IR-Based Home Security Sensor with Directional Antenna</td>
<td>950</td>
</tr>
<tr>
<td>Katsushi Ono, Yusei Noguchi, Youichiro Nakahata, Isamu Matsunami, Akihiro Kajiwara</td>
<td></td>
</tr>
<tr>
<td>Approaching Vehicle Detection Using Linear Microphone Array</td>
<td>955</td>
</tr>
<tr>
<td>Kenji Kodera, Akitoshi Itai, Hiroshi Yatsukawa</td>
<td></td>
</tr>
<tr>
<td>Saccade-Related EEG Signals by ICA Algorithms</td>
<td>961</td>
</tr>
<tr>
<td>Arao Funase, Motoaki Mouri, Tohru Yagi, Andrzej Cichocki, Ichi Takumi</td>
<td></td>
</tr>
<tr>
<td><strong>RELAY NETWORKS</strong></td>
<td></td>
</tr>
<tr>
<td>To Decode or To Amplify: Mix and Match for the Two-Way Two-Relay Network</td>
<td>966</td>
</tr>
<tr>
<td>Ping Hu, Kenneth W. Shum, Chi Wan Sung</td>
<td></td>
</tr>
<tr>
<td>The Multiuser Gaussian Parallel Relay Network</td>
<td>972</td>
</tr>
<tr>
<td>Chi Wan Sung, Ping Hu, Kin K. Leung</td>
<td></td>
</tr>
<tr>
<td>Bursty Narrowband Relay Networks in the Low-SNR Regime</td>
<td>978</td>
</tr>
<tr>
<td>Tony Q. S. Quek, Hyundong Shin</td>
<td></td>
</tr>
<tr>
<td>Achievable Rates and Schedules for Half Duplex Phase Fading Multiple-Relay Networks</td>
<td>984</td>
</tr>
<tr>
<td>Lawrence Ong, Wei Wang, Mehul Motani</td>
<td></td>
</tr>
<tr>
<td><strong>MIMO 3</strong></td>
<td></td>
</tr>
<tr>
<td>Rate Adaptive Modulation with MIMO Mode Switching Between Spatial Multiplexing and Diversity</td>
<td>990</td>
</tr>
<tr>
<td>Chanhong Kim, Jungwoo Lee</td>
<td></td>
</tr>
<tr>
<td>Vector Precoding for Singular MIMO Channels</td>
<td>996</td>
</tr>
<tr>
<td>Vesna Gardasevic, Ralf R. Müller, Finn F. Knudsen</td>
<td></td>
</tr>
<tr>
<td>Design of Low-Density Parity-Check Codes for Multi-Input Multi-Output Systems</td>
<td>999</td>
</tr>
<tr>
<td>Jeong Hwan Shin, Jin Young Kim, Jun Heo</td>
<td></td>
</tr>
<tr>
<td>A Multiplexed Transmission Scheme with Unequal Error Protection on MIMO Frequency Selective Channels</td>
<td>1003</td>
</tr>
<tr>
<td>Yukio Tsuchiya, Yasunori Iwanami, Eiji Okamoto, Keiichiro Hayakawa, Katsushi Sanda</td>
<td></td>
</tr>
<tr>
<td>Beamforming Design for the MIMO Downlink for Maximizing Weighted Sum-Rate</td>
<td>1009</td>
</tr>
<tr>
<td>Rajiv Agarwal, John M. Cioffi</td>
<td></td>
</tr>
<tr>
<td><strong>SECURITY APPLICATIONS</strong></td>
<td></td>
</tr>
<tr>
<td>A Note on the Error of Optimized LFC Private Information Retrieval Scheme</td>
<td>1015</td>
</tr>
<tr>
<td>Jin Tamura, Kazukuni Kobara, Ryo Nojima, Hideki Imai, Helger Lipmaa</td>
<td></td>
</tr>
<tr>
<td>Enhancing the Security of Bloom-Filters with Blind Signatures</td>
<td>1019</td>
</tr>
<tr>
<td>Ryo Nojima, Jin Tamura, Youki Kadoyayashi</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>HW-Based Random Bit Sequence Generation Method Using Gettime Function</td>
<td>1025</td>
</tr>
<tr>
<td>Kenji Yamaguchi, Katsuhiro Nakamura</td>
<td></td>
</tr>
<tr>
<td>The Practicality of the Keyword Search using PIR</td>
<td>1031</td>
</tr>
<tr>
<td>Rei Yoshida, Yang Cui, Rie Shigetomi, Hideki Imai</td>
<td></td>
</tr>
<tr>
<td>Improvement of Referrer SPAM Blocking System</td>
<td>1037</td>
</tr>
<tr>
<td>Yusuke Kimura, Atsunori Watanabe, Takashi Katoh, Bhed Bahadur Bista, Toyoo Takata</td>
<td></td>
</tr>
</tbody>
</table>

**CDMA**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Convergence Behaviors of Adaptive DS-CDMA Receivers</td>
<td>1043</td>
</tr>
<tr>
<td>Hsuan-Fu Wang, Fang-Biau Ueng, Jui-Chi Chang, Li-Der Jeng</td>
<td></td>
</tr>
<tr>
<td>A Novel DS/CDMA Receiver with Performance Analysis</td>
<td>1049</td>
</tr>
<tr>
<td>Jun-Da Chen, Fang-Biau Ueng, Hsuan-Fu Wang, Jui-Chi Chang, Li-Der Jeng</td>
<td></td>
</tr>
<tr>
<td>The Analytical Model of the WCDMA Interface with Priorities in the UMTS Network</td>
<td>1055</td>
</tr>
<tr>
<td>Maciej Stasiak, Janusz Wieviöra, Piotr Zwierzykowski</td>
<td></td>
</tr>
<tr>
<td>Error Correction Scheme for Multi-Carrier CDMA with Bi-Orthogonal Modulation</td>
<td>1061</td>
</tr>
<tr>
<td>Hirokazu Tanaka, Shoichiro Yamasaki, Miki Haseyama</td>
<td></td>
</tr>
<tr>
<td>An Asymptotically Full Rate Cooperative Communication Scheme for DS-CDMA Systems with Non-Orthogonal Codes</td>
<td>1067</td>
</tr>
<tr>
<td>Amila V. Kariyapperuma, Sadharman K. Jayaweera</td>
<td></td>
</tr>
</tbody>
</table>

**DECODING ALGORITHMS**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the Number of Search Centers of Chase-Like Bounded-Distance Decoding</td>
<td>1073</td>
</tr>
<tr>
<td>Yuansheng Tang, Xinmei Huang, Tingsu Yan, Ming Chen</td>
<td></td>
</tr>
<tr>
<td>APP Decoding of Non-Binary Block Codes on Gilbert-Elliott Channels Using Generalized Weight Polynomials</td>
<td>1077</td>
</tr>
<tr>
<td>Wayne Griffiths, Hans-Jurgen Zepernick, Manora Caldera</td>
<td></td>
</tr>
<tr>
<td>A Self-Orthogonal Code and its Maximum-Likelihood Decoder for Combined Channel Estimation and Error Protection</td>
<td>1083</td>
</tr>
<tr>
<td>Chia-Lung Wu, Po-Ning Chen, Yunsghsiang S. Han, Shih-Wei Wang</td>
<td></td>
</tr>
<tr>
<td>Priority-First Search Decoding for Convolutional Tail-Biting Codes</td>
<td>1089</td>
</tr>
<tr>
<td>Yunsghsiang S. Han, Ting-Yi Wu, Hung-Ta Pai, Po-Ning Chen, Shin-Lin Shieh</td>
<td></td>
</tr>
</tbody>
</table>

**LOSSLESS SOURCE CODING**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Randomness Test Based on T-Codes</td>
<td>1095</td>
</tr>
<tr>
<td>Kenji Hamano, Hironoske Yamamoto</td>
<td></td>
</tr>
<tr>
<td>On the Maximum Shannon Entropy of the Full State Space of a T-Code Decoder</td>
<td>1101</td>
</tr>
<tr>
<td>Ulrich Speidel</td>
<td></td>
</tr>
<tr>
<td>On the Sliding Window Variations of Antidictionary Data Compression Using Dynamic Suffix Trees</td>
<td>1105</td>
</tr>
<tr>
<td>Takahiro Ota, Hiroyoshi Morita</td>
<td></td>
</tr>
<tr>
<td>On the Optimality of Sliding Window Lempel-Ziv Algorithm with Side Information</td>
<td>1111</td>
</tr>
<tr>
<td>Tony Jacob, Rakesh K. Bansal</td>
<td></td>
</tr>
<tr>
<td>On the Redundancy of Modified Lempel-Ziv Parsing Algorithm for Markovian Source</td>
<td>1117</td>
</tr>
<tr>
<td>Katsuya Kobayashi, Bing Chang Koh, Tsutomu Kawabata</td>
<td></td>
</tr>
</tbody>
</table>
SIGNAL PROCESSING 3

A Study on a Distributed Verification Scheme and its Efficiency ................................. 112
Hiroshi Yamamoto, Hiroshi Toyosumi

Effectiveness of Global Signal Elimination from Environmental Electromagnetic Signals for Earthquake Prediction .......................................................... 1128
Motoaki Mouri, Arao Funase, Ichi Takumi, Andrzej Cichocki, Hiroshi Yasukawa, Masayasu Hata

Anomaly Detection of Environmental Electromagnetic Wave based on Time Fluctuation and Cross-Correlation in Magnetic Field Azimuth .................................................... 1134
Tokiya Sato, Ichi Takumi, Masayasu Hata, Hiroshi Yasukawa

A Consideration on Scaling Functions of Wavelets .......................................................... 1140
Hajime Sato

APPLICATIONS OF INFORMATION THEORY 1

On Digraph-Different Permutations ............................................................................... 1146
Gérard Cohen, Emanuela Fachini, János Körner

Bounds on Fixed-Length Post-Processing Functions for Stationary Biased Random Number Generators ............................................................................. 1149
Koji Nuida

Characterizing the Discrete Capacity Achieving Distribution with Peak Power Constraint at the Transition Points ........................................................................ 1155
Naresh Sharma, Shlomo Shamai (Shitz)

Achieving Near-Capacity on Large Discrete Memoryless Channels with Uniform Distributed Selected Input ................................................................. 1161
Amine Mezghani, Josef A. Nossek, Michel T. Ivrlac

MIMO 4

Impact of Dimension on Causal Equalization of the MIMO Two-Tap Channel ................. 1167
Sander Wahls, Holger Boche

Detection Method for Recognizing Number of Parallel Transmitted Symbols in MIMO Cognitive Wireless Communication ........................................ 1173
Osamu Takyu, Takeo Fujii, Yohtaro Umeda, Masao Nakagawa

Adaptive Lattice Reduction in MIMO Systems ................................................................ 1179
Mohammad Erfan Danesh Jafari, Hossein Najafi, Mohamed Oussuma Damen

Transmission Performance of Layered-Symbol Iterative Interference Cancellation for Single-Carrier MIMO Multiplexing ........................................ 1184
Akinori Nakajima, Hiroshi Kubo

KNAPSACK CRYPTOSYSTEMS

A New Class of Cryptosystems based on Chinese Remainder Theorem .......................... 1190
Yasuyuki Murakami, Kiyoko Katayanagi, Masao Kasahara

Effectiveness of Plaintext Encoding in Knapsack PKC .................................................. 1196
Tatsuo Douzono, Takeshi Nasako, Yasuyuki Murakami

A Note on Performance of Low-Density Attack for Several Knapsack PKCs .................. 1201
Yoshifumi Kataoka, Takeshi Nasako, Yasuyuki Murakami, Masao Kasahara
A Note on Security of Knapsack PKC using Plaintext Encoding over Finite Fields ........................................ 1207
  Takeshi Nasako, Yasuyuki Murakami

COMMUNICATION SYSTEMS 2

User Unsuppressible Protocol Sequences for Collision Channel without Feedback ......................................... 1213
  Chung Shue Chen, Kenneth W. Shum, Chi Wan Sung, Wing Shing Wong, Geir E. Øien

Performance Study of Selection Diversity Systems with Non-Identical Fading Branches ............................... 1219
  Vishwanatha R. Gowda, Kwok Hung Li, Kah Chan Teh

Exact Outage Probability Analysis of Distributed Cooperative Transmission .................................................. 1224
  Ernest Kurniawan, A. S. Madhukumar, Francois Chin

Impact of Interference on the Performance of Selection Based Parallel Multiuser Scheduling .............................. 1229
  Sung Sik Nam, Mohamed-Slim Alouini, Hong-Chuan Yang

ENCODING AND DECODING

An Efficient SAT Encoding of Circuit Codes ........................................................................................................ 1235
  Yury Chebiryak, Daniel Kroening

A Linear-Time Nearest-Point Algorithm for the Lattice \( \Lambda_n \) ................................................................. 1239
  Robby G. McKilliam, I. Vaughan L. Clarkson, Warren D. Smith, Barry G. Quinn

Finding Fountain Codes for Real-Time Data by Fixed Point Method ............................................................... 1244
  Tuomas Tirronen, Jorma Virtamo

Iterative Decoding of BDPSK Modulated LDPC Codes using Two-Symbol-Interval Observations ................. 1250
  Vu Thanh Nam, Pooi Yuen Kam, Yan Xin

CONSTRAINED CODING

Constraints for Two-Dimensional Recording Media ............................................................................................. 1255
  Hiroshi Kamabe

Consideration on Two Dimensional Constraint Codes with Honeycomb Structure ........................................... 1261
  Kenji Kai, Shogo Usami, Akira Watanabe, Tadashi Wadayama

Maximum Entropy Rate of Markov Sources for Systems with Non-Regular Constraints .................................... 1267
  Georg Boecherer, Valdemar da Rocha, Cecilio Pimentel, Rudolf Mathar

Perfect Classified Channel Retaining DC Balance for High-Throughput Communication .................................. 1273
  Hiroki Matsuoka, Kouichi Inoue, Hiroaki Nishi

SIGNAL PROCESSING 4

Mismatched Filter for Binary Code Compressed to Several Chips ................................................................. 1279
  Kazutaka Hamada, Masanori Shinriki

Roesser's Model Realization of 2-D FIR Lossless Transfer Matrices ............................................................. 1283
  Robert Wirski, Krzysztof Wawryn

Semidefinite Programming for Variable Notch FIR Filters .............................................................................. 1289
  Toma Miyata, Naoyuki Aikawa, Yasuyuki Nishida

An Improved Acoustic Interference Canceller using Optimized IIR/FIR Filter Banks ....................................... 1294
  Ali O. Abid Noor, Salina Abdul Samad, Aini Hussain
APPLICATIONS OF INFORMATION THEORY 2

On the Condition of $\varepsilon$-Transmissibility in Joint Source-Channel Coding for Mixed Sources and Mixed Channels ........................................................................................................................................... 1299
Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa

A Joint Source-Channel Coding Scheme for Transmission of Correlated Discrete Sources over a Gaussian Multiple Access Channel ........................................................................................................................................... 1305
R Rajesh, Vinod Sharma

A Generalization of the Log-Likelihood Function and Weighted Average in Gauss' Law of Error................................................................................................................................................................................................................................................................. 1311
Tatsuaki Wada, Hiroki Suyari

Period and Link Length of the Logistic Map over Integers ........................................................................................................................................................................................................................................................................... 1316
Takeru Miyazaki, Shunsuke Araki, Satoshi Uehara

FADING CHANNEL

Robust Adaptive Coding Schemes for Multipath Fading Channels ................................................................. 1321
Abd Rahim Mat Sidek, Ahmad Zuri Sha'ameri

Optimal Frame-Splitting Ratio Achieving Lowest BER over AWGN and Rayleigh Fading Channels with Distributed Antennas........................................................................................................................................................................................................................................................................... 1326
Makoto Yasutake, Jun Cheng, Chen Sun, Yoichiro Watanabe

Multi-Branch Switched Diversity with Adaptive Switching Thresholds ........................................................................................................................................................................................................................................................................... 1331
Haewoon Nam, Mohamed-Slim Alouini

The Maximum Achievable Array Gain under Physical Transmit Power Constraint...................................... 1337
Michel T. Ivrlac, Josef A. Nossek

UNCONDITIONAL SECURITY

New Bent Functions from Positive and Negative Functions of Old Bent Functions....................................... 1343
Joan-Josep Climent, Francisco J. Garcia, Verónica Requena

A Study on Occurrence Rates per Bit for the Logistic Map over Integers ...................................................... 1349
Shunsuke Araki, Takeru Miyazaki, Satoshi Uehara

A Cellular Automata Based HB#-Like Low Complexity Authentication Technique.............................................. 1354
Miodrag J. Mihaljevic, Hajime Watanabe, Hideki Imai

An Unconditionally Secure Protocol Based on Lattices over the Gaussian Channel .................................. 1360
Motohiko Isaka

TURBO AND CONVOLUTIONAL CODES

Tuned Turbo Codes ....................................................................................................................................................... 1366
Christian Koller, Alexandre Graell i Amat, Jörg Kliewer, Francesca Vatta, Daniel J. Costello Jr.

A Distance Spectrum Estimation Method of Turbo Codes ....................................................................................... 1372
Takakazu Sakai, Koji Shibata

Nonsystematic Turbo Codes: Design and Bounds on Effective Free Distance ................................................... 1377
Francesca Vatta, Alexandre Graell i Amat, Adrish Banerjee, Daniel J. Costello Jr.

On the Weight Distribution of Recursive Systematic Convolutional Codes .................................................. 1383
Hideki Yoshikawa
RELAY CHANNEL

Capacity of a More General Class of Relay Channels .................................................. 1388
Ghosheh Abed Hodtani, Mohammad Reza Aref

The Relay Channel with Partial Causal State Information ........................................ 1392
Majid N. Khormuji, Mikael Skoglund

Bounds on the Capacity of the Relay Channel with States at the Source .................. 1398
Abdellatif Zaidi, Luc Vandendorpe

Achievable Rates for Multiple Access Relay Channel with Generalized Feedback .... 1404
Chin Keong Ho, Kiran T. Gowda, Sumei Sun

SIGNAL PROCESSING 5

The Optimum Approximation of Signals Having Quite Small Side-Lobes .................. 1410
Yuichi Kida, Takuro Kida

Synthesis of Multidimensional Lossless Transfer Functions via Sum of Squares of
Polynomials .................................................................................................................. 1416
Robert Wirski

A Flexible Baseband Processor with Multi-Resolution Spectrum-Sensing Functionality .... 1422
Koh Tsuruda, Shintaro Izumi, Hyeokjong Lee, Takashi Takeuchi, Hiroshi Kawaguchi, Masahiko
Yoshimoto

A Study on Improving Image Quality of Highly Compressed Moving Pictures .......... 1428
Tomio Goto, Tatsuya Yamazaki, Masaru Sakurai

MULTI-TERMINAL INFORMATION THEORY 2

Signal Source Estimation in Sensor Networks ............................................................ 1434
Azadeh Vosoughi

Distributed Source Coding of Correlated Gaussian Observations ............................... 1440
Yasutada Oohama

On Tomlinson-Harashima Precoding in 2-User Degraded Gaussian Broadcast Channels .... 1446
Carolin Huppert, Martin Bossert

Correlated Gaussian Sources over Orthogonal Gaussian Channels ............................ 1452
R Rajesh, Vinod Sharma

SPACE TIME CODING

Maximal Orders in Space-Time Coding: Construction and Decoding ......................... 1458
Camilla Hollanti, Kalle Ranto

Diversity Embedded Space-Time Code from Quasi-Orthogonal Designs .................... 1463
Kiran T. Gowda, Chau Yuen, Sumei Sun

A Two-Hop Amplify-and-Forward Scheme for Extended Orthogonal Space-Time Coding
in Cooperative Networks ......................................................................................... 1469
Nasr Eltayeb, Shakiru Kassim, Jonathon Chambers

Hybrid ARQ for Non-Orthogonal Space-Time Block Codes ...................................... 1474
Rui Lin, Philippa A. Martin
Cooperative ARQ for Distributed Space-Time Coding: the Diversity-Multiplexing-Delay Tradeoff

Hsin-Li Chiu, Sau-Hsuan Wu

SYMmetric Key EncryPTION

Cryptanalysis of CLEFIA using Multiple Impossible Differentials

Yukiyasu Tsunoo, Etsuko Tsujihara, Maki Shigeri, Tomoyasu Suzaki, Takeshi Kawabata

A Method of Randomizing a Part of an FPGA Configuration Bitstream

Masaki Nakanishi, Yumiko Murakami

A Stream Cipher Design Based on Embedding of Random Bits

Miodrag J. Mihaljevic, Hideki Imai

The 32nd-Order Differential Attack on MISTY1 without FL Functions

Yasutaka Igarashi, Toshinobu Kaneko

COMMUNICATION SYSTEMS 3

Ranging Error of Ultra-Wideband Vehicle Radar

Isamu Matsunami, Youichiro Nakahata, Katsushi Ono, Akihiro Kajiwara

A Novel Primary-Secondary User Power Control Game for Cognitive Radios

Tianming Li, Sudharman K. Jayaweera

Estimation of Effective Earth Radius Factor Based on UHF Band Measurement

Masahiro Nishi, Tetsuya Amano, Teruaki Yoshida

Adaptive Key Generation in Secret Key Agreement Scheme based on the Channel Characteristics in OFDM

Shimpei Yasukawa, Hisato Iwai, Hideichi Sasaoka

LDPC CODES 5

On the Design of Irregular GLDPC Codes with Low Error Floor over the BEC

Enrico Paolini, Marc Fossorier, Marco Chiani

Code Design and Performance Analysis Using a 2-Level Generalized Tanner Graph on the Binary Erasure Channel

Eirik Rosnes

An Efficient Design of Irregular LDPC Codes using Beta Approximation for the Gilbert-Elliott Channel

Manabu Kobayashi, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa

Rate-Compatible Punctured LDPC Codes based on Recovery Tree

Sunghoon Choi, Kwangseok Noh, Jeong Hwan Shin, Jun Heo

SEQUENCES

Extension of Golay's Two Pair Construction for General Complex Complementary Sequences

Ying Li, Yen-Wen Huang

New Quaternary Low Correlation Zone Sequence Sets Constructed from Binary Low Correlation Zone Sequence Sets

Ji-Woong Jang, Sang-Hyo Kim
New Construction of p-ary Sequence Family with Large Linear Span ......................................................... 1562
Young-Sik Kim, Jung-Soo Chung, Jong-Seon No

On the Number of Distinct Autocorrelation Distributions of M-ary Sidel'nikov Sequences .......... 1565
Jung-Soo Chung, Young-Sik Kim, Jong-Seon No, Habong Chung

Crosscorrelation of m-Sequences with Decimation d=(p^l +1)/(p^k +1) ..................................................... 1569
Aina Johansen, Tor Helleseth

SIGNAL PROCESSING 6

Non-Uniform Sampling --- Signal and System Representation ................................................................. 1575
Holger Boche, Ullrich J. Mönich

Nonlinear Feedback Control of Stabilization Problem via Formal Linearization Using
Taylor Expansion ........................................................................................................................................... 1581
Kazuo Komatsu, Hitoshi Takata

Robust Interference Control Techniques for Cognitive Radios using Worst-Case
Performance Optimization ....................................................................................................................... 1586
Kanapathippillai Cumanan, Ranaji Krishna, Vimal Sharma, Sangarapillai Lambotharan

A Numerical Solution of Linear Variable-Coefficient Partial Differential Equations with
Two Independent Variables Based on Kida's Optimum Approximation Theory .............................. 1591
Yuichi Kida, Takuro Kida

MULTI-TERMINAL INFORMATION THEORY 3

Information Ambiguity .................................................................................................................................. 1597
Samar Agnihotri, H. S. Jamadagni

Reliability and Efficiency of Flexibly Decodable Distributed Coding Strategies .............................. 1603
Awlok Josan, David L. Neuhoff

An Application of Linear Codes to Slepian-Wolf Coding of Individual Sequences ................... 1608
Shigeaki Kuzuoka

Berger-Tung Problem: A Systematic Approach Based on Canonical Description .......................... 1614
Soumya Jana, Richard Blahut

Author Index