2018 International Symposium on Information Theory and Its Applications (ISITA 2018)

Singapore
28-31 October 2018

IEEE Catalog Number: CFP1805E-POD
ISBN: 978-1-5386-8223-4

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1805E-POD
ISBN (Print-On-Demand):	978-1-5386-8223-4
ISBN (Online):	978-4-88552-318-2

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

Monday, October 29

Monday, October 29 9:00 - 10:00

Mo-AM-P: Plenary Talk 1

Past, Present, and Future of Polar Coding
Alexander Vardy (University of California at San Diego)

Room: Waterfront ballroom
Chair: Pascal Vontobel (The Chinese University of Hong Kong, Hong Kong)

Monday, October 29 10:20 - 12:00

Mo-AM-1-1: Deletion / DNA Codes

Room 1 (Paradiso)
Chair: Han Mao Kiah (Nanyang Technological University, Singapore)

Cardinalities of BAD Correcting Codes
Takehiko Mori and Manabu Hagiwara (Chiba University, Japan)
pp. 1-5

An Improvement of Non-binary Code Correcting Single b-Burst of Insertions or Deletions
Toyohiko Saeki and Takayuki Nozaki (Yamaguchi University, Japan)
pp. 6-10

Formalization of Insertion / Deletion Codes and the Levenshtein Metric in Lean
Justin Kong (Chiba University, Japan); David Webb (University of Hawaii at Manoa, USA); Manabu Hagiwara (Chiba University, Japan)
pp. 11-15

Soft-Decision Decoding for DNA-Based Data Storage
Mu Zhang (Huawei Technologies Co., Ltd, P.R. China); Kui Cai (Singapore University of Technology and Design, Singapore); Kees A. Schouhamer Immink (Turing Machines Inc., The Netherlands); Pingping Chen (Fuzhou University, P.R. China)
pp. 16-20

On Constant GC-content Cyclic DNA Codes With Long Codewords
Ramy Taki ElDin (Ain Shams University, Egypt); Hajime Matsui (Toyota Technological Institute, Japan)
pp. 21-25

Mo-AM-1-2: Machine Learning (Invited Session)

Room 2 (Cardinal)
Chair: Takafumi Kanamori (Tokyo Institute of Technology, Japan)

Scalable Machine Learning on Compact Data Representations
Yasuo Tabei (RIKEN Center for Advanced Intelligence Project, Japan)
pp. 26-30

Fast yet Simple Natural-Gradient Descent for Variational Inference in Complex Models
Mohammad Emtiyaz Khan and Didrik Nielsen (RIKEN, Japan)
pp. 31-35

Introduction to Bandit Convex Optimization Algorithms
Wataru Kumagai (RIKEN, Japan)
pp. 36-39

Combinatorial Online Prediction
Kohei Hatano (Kyushu University & RIKEN AIP, Japan)
pp. 40-44

Mo-AM-1-3: Statistical Analysis

Room 3 (Galleria III)
Chair: Hiroshi Fujisaki (Kanazawa University, Japan)

Generalized Dirichlet-Process-Means for Robust and Maximum Distortion Criteria
Masahiro Kobayashi and Kazuho Watanabe (Toyohashi University of Technology, Japan)
pp. 45-49

Entropic Centrality for non-atomic Flow Networks
Frederique Oggier (Nanyang Technological University, Singapore); Silivanxay Phetsouvanh (NTU Singapore, Singapore); Anwitaman Datta (Nanyang Technological University, Singapore)
pp. 50-54

Convexity of mutual information along the Ornstein-Uhlenbeck flow
Andre Wibisono (Georgia Institute of Technology, USA); Varun Jog (University of Wisconsin - Madison, USA)
pp. 55-59

Sparse Bayesian Hierarchical Mixture of Experts and Variational Inference
Yuji Iikubo, Shunsuke Horii and Toshiyasu Matsushima (Waseda University, Japan)
pp. 60-64

On Enumerating Distributions for Associated Vectors in the Entropy Space
Mohammad Sultan Alam (Indian Institutue of Technology Mandi, India); Satyajit Thakor (Indian Institute of Technology Mandi, India); Syed Abbas (Indian Institutue of Technology Mandi, India)
pp. 65-69

Mo-AM-1-4: Signature Schemes

Room 4 (Falcon)
Chair: Bagus Santoso (The University of Electro-Communications, Japan)

Rank metric code-based signature
Chik How Tan, Theo Fanuela Prabowo and Terry Shue Chien Lau (National University of Singapore, Singapore)
pp. 70-74

A Generic Construction of an Identity-based Signature from a Sigma Protocol
Masayuki Fukumitsu (Hokkaido Information University, Japan); Shingo Hasegawa (Tohoku University, Japan)
pp. 75-79

Efficiency Improvement in Group Signature Scheme with Probabilistic Revocation
Nasima Begum (University of Asia Pacific, Bangladesh); Toru Nakanishi (Hiroshima University, Japan)
pp. 80-84

A Consideration on the Transformation from Deniable Group Signature to Disavowable PKENO
Ai Ishida, Yusuke Sakai and Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology, Japan)
pp. 85-89

Monday, October 29 14:00 - 15:40

Mo-PM-1-1: Index/Network Coding

Room 1 (Paradiso)
Chair: Tadashi Wadayama (Nagoya Institute of Technology, Japan)

Expected Error Rate of Probabilistic Network Codes over Gaussian Relay Network
Motohiko Isaka (Kwansei Gakuin University, Japan)
pp. 90-94

Reduced Dimensional Optimal Vector Linear Index Codes for Index Coding Problems with Symmetric Neighboring and Consecutive Side-information
Mahesh Babu Vaddi and B. Sundar Rajan (Indian Institute of Science, India)
pp. 95-99

Index Codes for Interlinked Cycle Structures with Outer Cycles
Karanam Bharadwaj (Indian Institute of Science, Bangalore, India); B. Sundar Rajan (Indian Institute of Science, India)

pp. 100-104

Optimal Scalar Linear Index Codes for Some Two-Sender Unicast Index Coding Problems
Chinmayananda Arunachala and B. Sundar Rajan (Indian Institute of Science, India)
pp. 105-109

On the Broadcast Rate of Index Coding Problems with Symmetric and Consecutive Interference
Mahesh Babu Vaddi and B. Sundar Rajan (Indian Institute of Science, India)
pp. 110-114

Mo-PM-1-2: Non-Asymptotic Information Theory (Invited Session)

Room 2 (Cardinal)
Chair: Vincent Y. F. Tan (National University of Singapore, Singapore)

Information Spectrum Analysis for Mismatched Decoding
Anelia Somekh-Baruch (Bar-Ilan University, Israel)
pp. 115-119

Privacy Amplification: Recent Developments and Applications
Wei Yang (Qualcomm Research, USA); Rafael F. Schaefer (Technische Universität Berlin, Germany); Vincent Poor (Princeton University, USA)
pp. 120-124

Asymptotics of the random coding union bound
Josep Font-Segura and Alfonso Martinez (Universitat Pompeu Fabra, Spain); Albert Guillén i Fàbregas (ICREA and Universitat Pompeu Fabra & University of Cambridge, Spain)
pp. 125-129

Connections Between the Error Probability and the r-wise Hamming Distances
Hsuan-Yin Lin (Simula UiB, Norway); Stefan M. Moser (ETH Zurich, Switzerland & National Chiao Tung University (NCTU), Taiwan); Po-Ning Chen (National Chiao Tung University, Taiwan)
pp. 130-134

Mo-PM-1-3: Communication Systems

Room 3 (Galleria III)
Chair: Kenji Nakagawa (Nagaoka University of Technology, Japan)

Detection of Noisy and Corrupted Data Using Clustering Techniques
Kui Cai (Singapore University of Technology and Design, Singapore); Kees A. Schouhamer Immink (Turing Machines Inc., The Netherlands)
pp. 135-138

Sparse Multiple Access and Code Design with Near Channel Capacity Performance
Akira Osamura, Guanghui Song and Jun Cheng (Doshisha University, Japan); Kui Cai (Singapore University of Technology and Design, Singapore)
pp. 139-143

Super Resolution Channel Estimation with Spread Spectrum Signal and Atomic Norm Minimization
Dongshin Yang and Yutaka Jitsumatsu (Kyushu University, Japan)
pp. 144-148

An Efficient Strategy for Applying Compute-and-Forward to the MARC
Mohammad Nur Hasan (Japan Advanced Institute of Science and Technology, Japan); Brian Michael Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan)
pp. 149-153

Block-error Threshold Analysis of Protographs in 5G-Standard
Asit Pradhan (Indian Institute of Technology Madras, India); Andrew Thangaraj (IIT Madras, India)
pp. 154-158

Mo-PM-1-4: Security Models and Protocols

Room 4 (Falcon)
Chair: Toru Nakanishi (Hiroshima University, Japan)

On the Anonymization of Differentially Private Location Obfuscation
Yusuke Kawamoto and Takao Murakami (National Institute of Advanced Industrial Science and Technology (AIST), Japan)
pp. 159-163

A Succinct Model for Re-identification of Mobility Traces Based on Small Training Data
Takao Murakami (National Institute of Advanced Industrial Science and Technology (AIST), Japan)
pp. 164-168

How to generate transparent random numbers using blockchain
Yuto Ehara (Media Entertainment Japan inc., Japan); Mitsuru Tada (Chiba University, Japan)
pp. 169-173

Decentralized Netting Protocol over Consortium Blockchain
Ken Naganuma (Hitachi, The University of Tokyo, Japan); Masayuki Yoshino (Hitachi, Ltd & The University of Tokyo, Japan); Hisayoshi Sato (Hitachi, Ltd., Japan); Nishio Yamada (Hitachi, Japan); Takayuki Suzuki (Hitachi, Ltd., Japan); Noboru Kunihiro (The University of Tokyo, Japan)
pp. 174-177

Mobile Forensics for Cloud Storage Service on iOS Systems
Cheng-Ta Huang (Oriental Institute of Technology, Taiwan); Shiuh-Jeng Wang (Central Police University, Taiwan); Hung-Jui Ko (University of Chung-Hsing, Taiwan)
pp. 178-182

Monday, October 29 16:00 - 17:40

Mo-PM-2-1: Lattice and Closest Vector Problem

Room 1 (Paradiso)
Chair: Jos H. Weber (Delft University of Technology, The Netherlands)

Shaping Gain of Lattices Based on Convolutional Codes and Construction A
Fan Zhou and Brian Michael Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan)
pp. 183-187

Reliability-Based Parametric LDLC Decoding
Warangrat Wiriya (Japan Advanced Institute of Science and Technology, Japan); Brian Michael Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan)
pp. 188-192

The Double-Plane Algorithm: A simple algorithm for the closest vector problem
Ferdinand Blomqvist and Marcus Greferath (Aalto University, Finland)
pp. 193-197

On quotient metrics and decoding problems
Ferdinand Blomqvist (Aalto University, Finland)
pp. 198-202

Further Results on the Error Correction Capability of Irregular LDPC Codes under the Gallager A Algorithm
Masanori Hirotomo (Saga University, Japan); Hiroto Tamiya (NEC Corporation, Japan); Masakatu Morii (Kobe University, Japan)
pp. 203-207

Mo-PM-2-2: Cryptographic Protocols (1)

Room 2 (Cardinal)
Chair: Mitsugu Iwamoto (The University of Electro-Communications, Japan)

Multi-party Key Exchange Protocols from Supersingular Isogenies
Satoshi Furukawa and Noboru Kunihiro (The University of Tokyo, Japan); Katsuyuki Takashima (Mitsubishi Electric, Japan)
pp. 208-212

Secure Hybrid Authentication Protocols against Malicious Key Generation Center
SeongHan Shin (AIST, Japan)
pp. 213-217

Mo-PM-2-3: Graph-Based Analysis / Network Coding

Room 3 (Galleria III)
Chair: Kazushi Mimura (Hiroshima city university, Japan)

Mo-PM-2-4: Error Probability Analysis

Room 4 (Falcon)
Chair: Shigeaki Kuzuoka (Wakayama University, Japan)

Tuesday, October 30

Tuesday, October 30 9:00 - 10:00

Tu-AM-P: Plenary Talk 2

Non-Convex Optimization and Multiuser Information Theory
Chandra Nair (The Chinese University of Hong Kong)

Room: Waterfront ballroom
Chair: Yasutada Oohama (University of Electro-Communications, Japan)

Tuesday, October 30 10:20 - 12:00

Tu-AM-1-1: Erasure Correction

Room 1 (Paradiso)
Chair: Prakash Chaki (NEC Corporation, Japan)

Erasure Correcting Codes by Using Shift Operation and Exclusive OR
Yuta Hanaki and Takayuki Nozaki (Yamaguchi University, Japan)
pp. 281-285

Efficient Scheduling of Serial Iterative Decoding for Zigzag Decodable Fountain Codes
Yoshihiro Murayama and Takayuki Nozaki (Yamaguchi University, Japan)
pp. 286-290

Shifted Coded Slotted ALOHA
Tomokazu Emoto and Takayuki Nozaki (Yamaguchi University, Japan)
pp. 291-295

On the Local Erasure Correction Capacity of Convolutional Codes
Fedor Ivanov and Alexey Kreshchuk (Institute for Information Transmission Problems & National Research University Higher School of Economics, Russia); Victor V. Zyablov (Institute for Information Transmission Problems (IITP) RAS, Russia)
pp. 296-300

Blind Reconstruction of Binary Cyclic Codes over Binary Erasure Channel
Arti Yardi (IRIT/ENSEEIHT, University of Toulouse, France)
pp. 301-305

Tu-AM-1-2: Practical Security

Room 2 (Cardinal)
Chair: Hidenori Kuwakado (Kansai University, Japan)

An Experimental Analysis on Lattice Attacks against Ring-LWE over Decomposition Fields
Shota Terada (Panasonic Corporation, Japan); Hideto Nakano and Shinya Okumura (Graduate School of Engineering, Osaka University, Japan); Atsuko Miyaji (Osaka University & Japan Advanced Institute of Science and Technology, Japan)
pp. 306-310

An Observation on the Randomness Assumption over Lattices
Tadanori Teruya (National Institute of Advanced Industrial Science and Technology, Japan)
pp. 311-315

An Analysis of a Defence Method against Slow HTTP DoS Attack
Tetsuya Hirakawa, Kanayo Ogura, Bhed Bahadur Bista and Toyoo Takata (Iwate Prefectural University, Japan)
pp. 316-320

A Watermarking Method for Embedding into the External Shapes of Objects
Hiroshi Yamamoto and Kazuki Sano (Tokai University, Japan)
pp. 321-325

Suitable Symbolic Models for Cryptographic Verification of Secure Protocols in ProVerif
Hiroyuki Okazaki (Shinshu University Graduate School, Japan); Yuichi Futa (School of Computer Science, Tokyo University of Technology, Japan); Kenichi Arai (Nagasaki University, Japan)
pp. 326-330

Tu-AM-1-3: Quantum Information (1)

Room 3 (Galleria III)
Chair: Pascal Vontobel (The Chinese University of Hong Kong, Hong Kong)

Exploring Quantum Supremacy in Access Structures of Secret Sharing by Coding Theory
Ryutaroh Matsumoto (Nagoya University, Japan)
pp. 331-333

Performance of Nonbinary Cubic Codes
Arun John Moncy and Pradeep K Sarvepalli (Indian Institute of Technology Madras, India)
pp. 334-338

Quantum Key Distribution using Extended Mean King's Problem
Ayumu Nakayama (Graduate School of Science and Engineering Chiba University, Japan); Masakazu Yoshida (University of Nagasaki, Japan); Jun Cheng (Doshisha University, Japan)
pp. 339-343

Error performance and robustness of optimum quantum detection for MPSK signals in the presence of phase noise
Tiancheng Wang (Aichi Prefectural University, Japan); Kenji Nakahira (Tamagawa University, Japan); Tsuyoshi Usuda (Aichi Prefectural University, Japan)
pp. 344-348

Tu-AM-1-4: Shannon Theory

Room 4 (Falcon)
Chair: Shun Watanabe (Tokyo University of Agriculture and Technology, Japan)

A Study on the Problem of Channel Resolvability for Channels with Countable Input Alphabet
Shigeaki Kuzuoka (Wakayama University, Japan)
pp. 349-353

Variable-Length Intrinsic Randomness Allowing Positive Value of the Average Variational Distance
Jun Yoshizawa, Shota Saito and Toshiyasu Matsushima (Waseda University, Japan)
pp. 354-358

New Results on Variable-Length Lossy Compression Allowing Positive Overflow and Excess Distortion Probabilities
Shota Saito (Waseda University, Japan); Hideki Yagi (University of Electro-Communications, Japan); Toshiyasu Matsushima (Waseda University, Japan)
pp. 359-363

Overflow Probability of Codeword Cost in Variable-Length Coding Problem Allowing Non-Vanishing Error Probability
Ryo Nomura (Senshu University, Japan); Hideki Yagi (University of Electro-Communications, Japan)
pp. 364-368

Achievable Rate Regions for Source Coding with Delayed Partial Side Information
Tetsunao Matsuta and Tomohiko Uyematsu (Tokyo Institute of Technology, Japan)
pp. 369-373

Tuesday, October 30 14:00 - 15:00

Tu-PM-P: Tutorial Plenary

Innovation in Constrained Codes
Kees Schouhamer Immink (Turing Machines Inc.)

Room: Waterfront ballroom
Chair: Mehul Motani (National University of Singapore, Singapore)

Tuesday, October 30 15:20 - 16:20

Tu-PM-1-1: LDPC Codes

Room 1 (Paradiso)

Chair: Takayuki Nozaki (Yamaguchi University, Japan)

Structured Concatenation of Protograph LDPC Codes and Markers for Insertion/Deletion Channels
Ryo Shibata, Gou Hosoya and Hiroyuki Yashima (Tokyo University of Science, Japan)
pp. 374-378

Error Floor Estimation of Spatially-Coupled Irregular LDPC Code Ensembles
Kengo Shibata (NTT Advanced Technology, Japan); Shan Lu (Gifu University, Japan); Masakazu Yoshida (University of Nagasaki, Japan); Krishna Narayanan (Texas A&M University, USA); Jun Cheng (Doshisha University, Japan)
pp. 379-383

On the Decoding Radius Realized by Low-Complexity Decoded Non-Binary Irregular LDPC Codes
Pavel Rybin (IITP RAS & Skoltech, HSE, Russia); Alexey A. Frolov (Skolkovo Institute of Science and Technology & IITP RAS, Russia)
pp. 384-388

Tu-PM-1-2: Post-Quantum Cryptography (Invited Session)

Room 2 (Cardinal)
Chair: Noboru Kunihiro (The University of Tokyo, Japan)

An Improvement on the Linear Algebraic Attack for the Indeterminate Equation Encryption Scheme
Yasuhiko Ikematsu (The University of Tokyo, Japan); Koichiro Akiyama (Toshiba Corporation, Japan); Tsuyoshi Takagi (The University of Tokyo, Japan)
pp. 389-393

A New Three-Pass Code-based Zero-Knowledge Identification Scheme with Cheating Probability of Exactly Half
Bagus Santoso (The University of Electro-Communications, Japan); Taiyo Yamaguchi (University of Electro-Communications, Japan)
pp. 394-398

LPS-type Ramanujan Graphs
Hyungrok Jo (The University of Tokyo, Japan); Yoshinori Yamasaki (Ehime University, Japan)
pp. 399-403

Tu-PM-1-3: Applications of Information Theory

Room 3 (Galleria III)
Chair: Tetsuya Kojima (National Institute of Technology, Tokyo College, Japan)

Investigation of the Processors Evolution Using the Computer Capacity
Boris Ryabko (Institute of Computational Technologies of SB RAS & Novosibirsk State University, Russia); Anton Rakitskiy (Siberian State University of Telecommunication and Computer Science & ICT SB RAS, Russia)
pp. 404-408

Adaptive Notch Howling Canceller Using Group Delay Information
Nobuhiro Mikami (Tokyo University of Science, Japan); Kanji Mashita (Jvckenwood Corporation, Japan); Naoyuki Aikawa (Tokyo University of Science, Japan)
pp. 409-412

Chaos-Based Stream Cipher Using a Star Network of Chaotic Maps
Takaya Miyano and Kenichiro Cho (Ritsumeikan University, Japan)
pp. 413-417

Tu-PM-1-4: Compressed Sensing

Room 4 (Falcon)
Chair: Junichi Takeuchi (Kyushu University, Japan)

Variational Bayes method for matrix factorization to two sparse factorized matrices
Tomoki Tamai and Koujin Takeda (Ibaraki University, Japan)
pp. 418-422

Recovery Guarantee of Sparse Binary Sensing Matrices under Greedy Algorithm

Wen-Yao Chen and Chung-Chin Lu (National Tsing Hua University, Taiwan)
pp. 423-426

Typical Performance of Sparse Signal Recovery from a Linear Measurement with Large Coherence
Minori Ihara and Kazunori Iwata (Hiroshima City University, Japan); Nobuo Suematsu (Hiroshima City University & Graduate School of Information Sciences, Japan); Kazushi Mimura (Hiroshima city university, Japan)
pp. 427-431

Tuesday, October 30 16:30 - 17:30

Tu-PM-2-1: Polar Codes

Room 1 (Paradiso)
Chair: Alexander Vardy (University of California San Diego, USA)

Improving Polar Codes by Spatial Coupling
Kai-Hsin Wang (National Tsing Hua University, Taiwan); Wei Hou (Xidian University, P.R. China); Shan Lu (Gifu University, Japan); Ping-Yuen Wu and Yeong-Luh Ueng (National Tsing Hua University, Taiwan); Jun Cheng (Doshisha University, Japan)
pp. 432-436

On the Properties of Bit-Reversal Shortening in Polar Codes
Prakash Chaki and Norifumi Kamiya (NEC Corporation, Japan)
pp. 437-441

Efficient SC Decoding of Convolutional Polar Codes
Ruslan Morozov (Saint-Petersburg State Polytechnical University, Russia); Peter Trifonov (Saint-Petersburg Polytechnic University, Russia)
pp. 442-446

Tu-PM-2-2: Symmetric Key Cryptography

Room 2 (Cardinal)
Chair: Tadanori Teruya (National Institute of Advanced Industrial Science and Technology, Japan)

Integral Cryptanalysis of Reduced-round KASUMI
Nobuyuki Sugio (NTT DOCOMO, INC., Japan); Yasutaka Igarashi and Toshinobu Kaneko (Tokyo University of Science, Japan)
pp. 447-451

Revisited Diffusion Analysis of Salsa and ChaCha
Yusuke Matsuoka (Osaka Univ, Japan); Atsuko Miyaji (Osaka University & Japan Advanced Institute of Science and Technology, Japan)
pp. 452-456

Parallelizable Message Preprocessing for Merkle-Damgard Hash Functions
Hidenori Kuwakado (Kansai University, Japan); Shoichi Hirose (The University of Fukui, Japan); Masahiro Mambo (Kanazawa University, Japan)
pp. 457-461

Tu-PM-2-3: Quantum Information (2)

Room 3 (Galleria III)
Chair: Masakazu Yoshida (University of Nagasaki, Japan)

Semi-Quantum Key Distribution with Limited Measurement Capabilities
Walter O Krawec (University of Connecticut, USA); Eric P Geiss (Iona College, USA)
pp. 462-466

Effect of Non-Symmetric Loss on Quantum Reading Using a Quasi-Bell State
Keita Ishikawa, Tiancheng Wang and Tsuyoshi Usuda (Aichi Prefectural University, Japan)
pp. 467-471

Applying a symmetrization method by coding to non-symmetric mixed-state signals
Souichi Takahira and Tsuyoshi Usuda (Aichi Prefectural University, Japan)
pp. 472-475

Tu-PM-2-4: Sequences

Room 4 (Falcon)

Chair: Hiroshi Kamabe (Gifu University, Japan)

A Novel Construction of Quadtree-Structured Zero-Correlation Zone Sequence Sets
Takafumi Hayashi (Niigata University, Japan); Anh T. Pham (The University of Aizu, Japan); Kensaku Kawauchi and Yoshinobu Tanno (National University of Singapore, Singapore); Shinya Matsufuji (Yamaguchi University, Japan); Takao Maeda (University of Aizu, Japan)
pp. 476-480

Hadamard-type Matrices on Finite Fields and Their Applications to Sequence Generation
Tetsuya Kojima (National Institute of Technology, Tokyo College, Japan)
pp. 481-485

A Study on Computational Methods of the Logistic Map over Integers for a Pseudorandom Number Generator
Shunsuke Araki and Hideyuki Muraoka (Kyushu Institute of Technology, Japan); Takeru Miyazaki and Satoshi Uehara (The University of Kitakyushu, Japan); Ken'ichi Kakizaki (Kyushu Institute of Technology, Japan)
pp. 486-490

Wednesday, October 31

Wednesday, October 31 9:00 - 10:00

We-AM-Poster: Recent Results Poster Session

Room: Waterfront ballroom

Code Parameter Estimation from Noisy Data: TPC   N/A
Swaminathan Ramabadran (Nanyang Technological University Singapore, Singapore); A S Madhukumar (Nanyang Technological University, Singapore)

Improved LT Code Degree Distribution and its Performance Evaluation   N/A
Takumi Ishiyama, Ryo Shibata, Gou Hosoya and Hiroyuki Yashima (Tokyo University of Science, Japan)

Probabilistic Shaping for BICM with Pseudorandom Sequence   N/A
Masashi Yuri, Ryo Shibata, Gou Hosoya and Hiroyuki Yashima (Tokyo University of Science, Japan)

Attack on Multiple-Use Password Protected Secret Sharing   N/A
Taiyu Kamiyama (Sophia University, Japan); Yuta Ugaya (University of Sophia, Japan); Keisuke Kodaira (Sophia University, Japan); Tomoharu Shibuya (Sophia University & Faculty of Science and Technology, Japan)

Consideration on b-weight for cyclic codes over b-symbol read channels   N/A
Yuto Kono and Shogo Usami (Meijo University, Japan)

Enumeration of Compact Trees of AIFV Codes   N/A
Kengo Hashimoto and Ken-ichi Iwata (University of Fukui, Japan); Hirosuke Yamamoto (Meiji University, Japan)

Some properties of NTU sequences   N/A
Gangsan Kim and Hong-Yeop Song (Yonsei University, Korea)

A Thresholded Discriminative Metric Learning Approach for Deep Speaker Recognition   N/A
Yin-Cheng Yeh, Yen-Chin Liao and Hsie-Chia Chang (National Chiao Tung University, Taiwan)

Security of K(AII) ΣΠ PKC Along with a Challenge Problem   N/A
Yasuyuki Murakami (Osaka Electro-Communication University, Japan); Masao Kasahara (Waseda University)

A p-adic Analysis of Periodic Properties for Knuth's Quadratic Congruence Sequences   N/A
Takeru Miyazaki (The University of Kitakyushu, Japan); Shunsuke Araki (Kyushu Institute of Technology, Japan); Kohei Kawase (The University of Kitakyushu, Japan); Hideyuki Muraoka (Kyushu Institute of Technology, Japan); Yasuyuki Nogami (Okayama University, Japan); Satoshi Uehara (The University of Kitakyushu, Japan)

Capacity Analysis for Hybrid FSO/RF Networks   N/A
Shubha Sharma and A S Madhukumar (Nanyang Technological University, Singapore);

Swaminathan Ramabadran (Nanyang Technological University Singapore, Singapore)

Evaluation of Leakage Information on Searchable Encryption Database N/A
Masayuki Yoshino (Hitachi, Ltd & The University of Tokyo, Japan); Ken Naganuma (Hitachi, The University of Tokyo, Japan); Noboru Kunihiro and Sota Onozawa (The University of Tokyo, Japan)

Channel Model Divided into Cylinder for Free-Space Optical Links in Rain N/A
Kyohei Futami, Gou Hosoya and Hiroyuki Yashima (Tokyo University of Science, Japan)

Performance Evaluation of Post-Quantum Cryptographic Algorithms using JavaScript N/A
Ye Yuan and Junting Xiao (Kyushu University, Japan); Kazuhide Fukushima and Shinsaku Kiyomoto (KDDI R&D Laboratories Inc., Japan); Tsuyoshi Takagi (The University of Tokyo, Japan)

Neural Network Detection of LDPC-Coded Random Access CDMA Systems N/A
Yuto Ichiki (University of Doshisha, Japan); Guanghui Song and Kui Cai (Singapore University of Technology and Design, Singapore); Shan Lu (Gifu University, Japan); Jun Cheng (Doshisha University, Japan)

Joint Secure Communication and Independent Random Number Generation against Eavesdropper N/A
Natsuki Hirotani, Tomohiko Uyematsu and Tetsunao Matsuta (Tokyo Institute of Technology, Japan)

Fundamental Trade-off among Identification, Secrecy and Template Rates in Identification System N/A
Vamoua Yachongka and Hideki Yagi (University of Electro-Communications, Japan)

A novel Doppler resistant low complexity CS-CDMA system N/A
Hikaru Mizuyoshi (The University of Electro-Communications, Japan); Chenggao Han (University of Electro-Communications, Japan)

A New Bound of (r,δ)-Locally Repairable Codes over Finite Field of Small Order N/A
Tomoya Hamada (The University of Electro-Communications, Japan); Hideki Yagi (University of Electro-Communications, Japan)

A Calculation Method using DFT Matrix for Roos Bound N/A
Junru Zheng (Kyushu Women's University, Japan); Takayasu Kaida (Kindai University, Japan)

Expected Graph Evolution for Spatially ``Mt. Fuji'' Coupled LDPC Codes N/A
Yuta Nakahara and Toshiyasu Matsushima (Waseda University, Japan)

Study the Quantitative Bound of Required Samples in Attacking GACD-based FHE Schemes N/A
Yuntao Wang (The University of Tokyo, Japan); Xiaoling YU (Nanjing University of Science and Technology & The University of Tokyo, Japan); Tsuyoshi Takagi (The University of Tokyo, Japan)

A Construction of Secret Sharing Schemes with Threshold 3 for Countably Infinite Participants N/A
Takashi Hisatome and Hiroki Koga (University of Tsukuba, Japan)

Generating Binary Quasi-Cyclic Reversible Codes N/A
Ramy Taki ElDin (Ain Shams University, Egypt); Hajime Matsui (Toyota Technological Institute, Japan)

Some Properties of Z 4 Sequences Obtained from Two Binary NTU A Sequences by the Gray Coding N/A
Masahiro Goto, Takeru Miyazaki and Satoshi Uehara (The University of Kitakyushu, Japan); Yasuyuki Nogami (Okayama University, Japan)

Research on Convolutional Codes for Dependable Storage Systems N/A
Tianyi Zhang (Chiba University, Japan)

Probability Density Based Performance Analysis for Energy Harvesting Communications N/A
Yu Morishima (National Institute of Technology, Suzuka College, Japan)

Detailed experimentation know-how about CPA against lightweight cipher implemented 8-bit microcontroller for tamper resistance test bench N/A
Arimitsu Shikoda, Hideki Yoshikawa, Masahiro Kaminaga, Toshinori Suzuki, Kota Kanou, Tsukasa Adachi, Jun Sato and Masaharu Fukase (Tohoku Gakuin University, Japan)

Dispensing with Noise Forward in the ``Weak'' Relay Eavesdropper Channel **N/A**
Krishnamoorthy Iyer (IIT Bombay, India)

A Note on a Bound on the Rate of a Locally Recoverable Code with Multiple Recovering Sets **N/A**
Koki Kazama and Akira Kamatsuka (Waseda University, Japan); Takahiro Yoshida (Yokohama College of Commerce, Japan); Toshiyasu Matsushima (Waseda University, Japan)

Asymptotic Analysis of Classification in the Presence of Generalized Label Noise **N/A**
Goki Yasuda, Tota Suko and Toshiyasu Matsushima (Waseda University, Japan)

A study of error-control scheme for WBAN based on retransmission **N/A**
Takahiro Goto (Yokohama National University, Japan); Kento Takabayashi (Okayama Prefectural University, Japan); Ryuji Kohno (Yokohama National University & University of Oulu, Japan)

Wednesday, October 31 10:20 - 12:00

We-AM-1-1: Coding for Various Models

Room 1 (Paradiso)
Chair: Manabu Hagiwara (Chiba University, Japan)

Reducing the Average Delay in Gradient Coding
Ming Hui Jovan Lee, Ivan Tjuawinata and Han Mao Kiah (Nanyang Technological University, Singapore)
pp. 491-495

Some classes of systematic polynomial codes correcting single- and adjacent transposition errors
Yanling Chen (University of Duisburg-Essen, Germany); Han Vinck (University of Duisburg-Essen & University of Johannesburg, Germany)
pp. 496-500

Codes for Endurance-Limited Memories
Yeow Meng Chee (Nanyang Technological University, Singapore); Michal Horovitz (Tel-Hai College, Upper Galilee & The Galilee Research Institute - Migal, Upper Galilee, Israel); Alexander Vardy (University of California San Diego, USA); Van Khu Vu (Nanyang Technological University, Singapore); Eitan Yaakobi (Technion, Israel)
pp. 501-505

Time-Varying Variable-Length Error-Correcting Codes
Victor Buttigieg and Johann A. Briffa (University of Malta, Malta)
pp. 506-510

Tree-Search Decoding Using Reduced-Size Stacks
Hsiang-Shun Shih, Chih-Shin Wang, Chia-Chun Chen and Mao-Chao Lin (National Taiwan University, Taiwan)
pp. 511-515

We-AM-1-2: Cryptographic Protocols (2)

Room 2 (Cardinal)
Chair: Yuji Suga (Internet Initiative Japan Inc., Japan)

On Hiding Access Timings in ORAM
Yuma Kanai and Kazuki Yoneyama (Ibaraki University, Japan)
pp. 516-519

Improved Verifiable Delegated Private Set Intersection
Shintaro Terada and Kazuki Yoneyama (Ibaraki University, Japan)
pp. 520-524

Tree-based Secure Comparison of Secret Shared Data
Hiraku Morita, Nuttapong Attrapadung, Satsuya Ohata and Shota Yamada (AIST, Japan); Koji Nuida (The University of Tokyo, Japan); Goichiro Hanaoka (AIST, Japan)
pp. 525-529

Secure Division Protocol and Applications to Privacy-preserving Chi-squared Tests
Hiraku Morita, Nuttapong Attrapadung and Satsuya Ohata (AIST, Japan); Koji Nuida (The University of Tokyo, Japan); Shota Yamada (AIST, Japan); Kana Shimizu (Waseda University,

Japan); Goichiro Hanaoka (AIST, Japan); Kiyoshi Asai (The University of Tokyo, Japan)
pp. 530-534

Accuracy/Efficiency Trade-Off for Privacy-Preserving Division Protocol
Satsuya Ohata, Hiraku Morita and Goichiro Hanaoka (AIST, Japan)
pp. 535-539

We-AM-1-3: Data Compression

Room 3 (Galleria III)
Chair: Ken-ichi Iwata (University of Fukui, Japan)

A Consideration on Classification of Extended Binary Memoryless Sources Under Which Distinct Huffman Codes Are Constructed
Nozomi Miya (Aoyama Gakuin University, Japan); Takahiro Yoshida (Yokohama College of Commerce, Japan); Hajime Jinushi (Aoyama Gakuin University, Japan)
pp. 540-544

Dynamic AIFV Coding
Tomotaka Hiraoka (Nochu Information System Co., Ltd., Japan); Hirosuke Yamamoto (Meiji University, Japan)
pp. 545-549

A Note on Lempel-Ziv Parser Tails and Substring Lengths
T. Aaron Gulliver (University of Victoria, Canada); Ulrich Speidel (University of Auckland, New Zealand); Niko Rebenich (University of Victoria, Canada)
pp. 550-554

Compression by Substring Enumeration with a Finite Alphabet Using Sorting
Takahiro Ota (Nagano Prefectural Institute of Technology, Japan); Hiroyoshi Morita (The University of Electro-Communications, Japan); Akiko Manada (Shonan Institute of Technology, Japan)
pp. 555-559

We-AM-1-4: Multiuser Information Theory

Room 4 (Falcon)
Chair: Hideki Yagi (University of Electro-Communications, Japan)

Novel Signal-Code Construction for Multiple Access System over Vector-Disjunctive Channel
Fedor Ivanov (Institute for Information Transmission Problems & National Research University Higher School of Economics, Russia); Pavel Rybin (IITP RAS & Skoltech, HSE, Russia)
pp. 560-564

Recursive Construction of k-Ary Uniquely Decodable Codes for Multiple-Access Adder Channel
Shan Lu (Gifu University, Japan); Wei Hou (Xidian University, P.R. China); Jun Cheng (Doshisha University, Japan); Hiroshi Kamabe (Gifu University, Japan)
pp. 565-569

Contributions to Successive Decoding for Multiple Access Channels
Lóránt Farkas and Tamás Kói (Budapest University of Technology and Economics, Hungary)
pp. 570-574

Slepian-Wolf Coding with Side-Information Having Insertion/Deletion Errors
Haruhiko Kaneko (Tokyo Institute of Technology, Japan)
pp. 575-579

Multi-terminal codes using constrained-random-number generators
Jun Muramatsu (NTT Corporation, Japan); Shigeki Miyake (NTT, Japan)
pp. 580-584

Wednesday, October 31 13:30 - 15:10

We-PM-1-1: Bounds and Metrics

Room 1 (Paradiso)
Chair: Motohiko Isaka (Kwansei Gakuin University, Japan)

Improved Asymptotic Sphere-Packing Bounds for Subblock-Constrained Codes
Anshoo Tandon (National University of Singapore, Singapore); Han Mao Kiah (Nanyang Technological University, Singapore); Mehul Motani (National University of Singapore, Singapore)
pp. 585-589

Lower Bound-oriented Parameter Calculation for AN coding
Juliana Hildebrandt, Till Kolditz, Dirk Habich and Wolfgang Lehner (Technische Universität Dresden, Germany)
pp. 590-594

Arbitrarily Low Redundancy Construction of Balanced Codes Using Realistic Resources
Danny Dubé (Université Laval, Canada)
pp. 595-599

An Upper Bound on the Generalized Cayley Distance
Akira Yamawaki, Hiroshi Kamabe and Shan Lu (Gifu University, Japan)
pp. 600-604

Properties of Binary Pearson Codes
Jos H. Weber (Delft University of Technology, The Netherlands); Kees A. Schouhamer Immink (Turing Machines Inc., The Netherlands)
pp. 605-609

We-PM-1-2: Cryptanalysis

Room 2 (Cardinal)
Chair: Masayuki Yoshino (Hitachi, Ltd & The University of Tokyo, Japan)

Equivalent Secret Key Attack against Knapsack PKC based on Subset Sum Decision Problem
Ryuichi Sakai and Yasuyuki Murakami (Osaka Electro-Communication University, Japan)
pp. 610-613

Security of Knapsack Cryptosystem Using Subset-Sum Decision Problem against Alternative-Solution Attack
Yasuyuki Murakami and Ryuichi Sakai (Osaka Electro-Communication University, Japan)
pp. 614-617

Side-Channel Attack using Order 4 Element against Curve25519 on ATmega328P
Yoshinori Uetake and Akihiro Sanada (Okayama University, Japan); Léo Weissbart (Grenoble INP-Esisar : Advanced Systems and Networks, France); Takuya Kusaka (Okayama University, Japan); Sylvain Duquesne (Université Rennes I, France); Yasuyuki Nogami (Okayama University, Japan)
pp. 618-622

A Study on the Parameter Size of the Montgomery Trick for ECDLP
Ken Ikuta (OKAYAMA University, Japan); Sho Joichi, Kazuya Kobayashi, Md. Al-Amin Khandaker, Takuya Kusaka and Yasuyuki Nogami (Okayama University, Japan)
pp. 623-627

A Study on the Parameter of the Distinguished Point Method in Pollard's Rho Method for ECDLP
Ken Ikuta (OKAYAMA University, Japan); Sho Joichi, Kazuya Kobayashi, Md. Al-Amin Khandaker, Takuya Kusaka and Yasuyuki Nogami (Okayama University, Japan)
pp. 628-632

We-PM-1-3: Data Compression and Related Topics

Room 3 (Galleria III)
Chair: Takahiro Ota (Nagano Prefectural Institute of Technology, Japan)

Examples of Formal Proofs about Data Compression
Reynald Affeldt (National Institute of Advanced Industrial Science and Technology, Japan); Jacques Garrigue and Takafumi Saikawa (Nagoya University, Japan)
pp. 633-637

Probability Approximation in Asymmetric Numeral Systems
Hidetoshi Yokoo and Toshiki Shimizu (Gunma University, Japan)
pp. 638-642

Invariant Measures for the Subshifts Associated with the Asymmetric Binary Systems

Hiroshi Fujisaki (Kanazawa University, Japan)
pp. 643-647

On Minimum Expected Length Prefix Codes Satisfying a (d,k) Runlength-Limited Constraint
Shivkumar K Manickam and Navin Kashyap (Indian Institute of Science, India)
pp. 648-652

We-PM-1-4: Information Theoretic Security / Multiterminal

Room 4 (Falcon)
Chair: Tetsunao Matsuta (Tokyo Institute of Technology, Japan)

On the Capacity of State-Dependent Gaussian Z-Interference Channel
Shahab Ghasemi-Goojani (KTH Royal Institute of Technology, Sweden); Panagiotis Papadimitratos (KTH, Sweden)
pp. 653-657

State-Dependent Gaussian Broadcast Channel with Common State Reconstructions
Viswanathan Ramachandran (Indian Institute of Technology Bombay, India); Meghna Sreenivasan and Sibi Raj B Pillai (IIT Bombay, India); Vinod M Prabhakaran (Tata Institute of Fundamental Research, India)
pp. 658-662

On the Secrecy Capacity of 2-user Gaussian Interference Channel with Independent Secret Keys
Aditya Sinha (Indian Institute of Technology Kharagpur, India); Parthajit Mohapatra (Indian Institute of Technology Tirupati, India); Jemin Lee (Daegu Gyeongbuk Institute of Science and Technology (DGIST), Korea); Tony Q. S. Quek (Singapore University of Technology and Design, Singapore)
pp. 663-667

Secrecy Performance on Half-Duplex Two-Way Multi-Relay Transmission Technique Under Wireless Physical Layer Security
Mohammed Ahmed Salem (Multimedia University (MMU), Malaysia); Azlan Abdul Aziz (Multimedia University, Melaka, Malaysia); Mohamad Yusoff Alias (Multimedia University, Malaysia); Abdul Aziz Abdul Rahman (Telekom Research & Development, Malaysia)
pp. 668-672

The Symmetric Two-hop Channel with an Untrusted Relay
Shahab Ghasemi-Goojani (KTH Royal Institute of Technology, Sweden); Panagiotis Papadimitratos (KTH, Sweden)
pp. 673-677

Wednesday, October 31 15:30 - 16:50

We-PM-2-1: Applications of Algebraic Coding

Room 1 (Paradiso)
Chair: Hajime Matsui (Toyota Technological Institute, Japan)

New Locator Polynomials for Cyclic Codes
Chong-Dao Lee (I-Shou University, Taiwan)
pp. 678-682

Joint Reconstruction of Reed-Solomon Encoder and Convolutional Interleaver in a Noisy Environment
Swaminathan Ramabadran (Nanyang Technological University Singapore, Singapore); A S Madhukumar (Nanyang Technological University, Singapore); Guohua Wang and Shang Kee Ting (Temasek Labs @ Nanyang Technological University, Singapore)
pp. 683-687

Some Constructions of Optimal Locally Repairable Codes
Wentu Song and Kui Cai (Singapore University of Technology and Design, Singapore)
pp. 688-692

Shortened Cyclic Codes for Correcting and Detecting Burst Errors
Roy D. Cideciyan, Simeon Furrer and Mark Lantz (IBM Zurich Research Laboratory, Switzerland)
pp. 693-697

We-PM-2-2: Public-Key Cryptography

Room 2 (Cardinal)
Chair: Kazuki Yoneyama (Ibaraki University, Japan)

A New Key Encapsulation Combiner
Takahiro Matsuda and Jacob Schuldt (AIST, Japan)
pp. 698-702

A Remark on an Identity-Based Encryption Scheme with Non-interactive Opening
Yusuke Sakai and Goichiro Hanaoka (AIST, Japan)
pp. 703-706

Generic Construction of Adaptively Secure Anonymous Key-Policy Attribute-Based Encryption from Public-Key Searchable Encryption
Junichiro Hayata (The University of Tokyo & AIST, Japan); Masahito Ishizaka (The University of Tokyo, Japan); Yusuke Sakai and Goichiro Hanaoka (AIST, Japan); Kanta Matsuura (University of Tokyo, Japan)
pp. 707-711

Embedding Lemmas for Functional Encryption
Ryo Kato (Panasonic, Japan); Naohisa Nishida, Ryo Hirano and Tatsumi Oba (Panasonic Corporation, Japan); Yuji Unagami (Panasonic Co., Japan); Shota Yamada and Tadanori Teruya (National Institute of Advanced Industrial Science and Technology, Japan); Nuttapong Attrapadung, Takahiro Matsuda and Goichiro Hanaoka (AIST, Japan)
pp. 712-716

We-PM-2-3: Fundamentals of Information Theory

Room 3 (Galleria III)
Chair: Jun Muramatsu (NTT Corporation, Japan)

Asymptotic Behavior of Typical Sets and the Smallest High Probability Set
Munenori Eto, Masanori Kawakita and Junichi Takeuchi (Kyushu University, Japan)
pp. 717-721

Second-Order Optimal Test in Composite Hypothesis Testing
Shun Watanabe (Tokyo University of Agriculture and Technology, Japan)
pp. 722-726

Generalized Fano-Type Inequality for Countably Infinite Systems with List-Decoding
Yuta Sakai (University of Fukui, Japan)
pp. 727-731

Analysis for the Slow Convergence in Arimoto Algorithm
Kenji Nakagawa (Nagaoka University of Technology, Japan); Yoshinori Takei (National Institute of Technology, Akita College, Japan); Kohei Watabe (Nagaoka University of Technology, Japan)
pp. 732-736

We-PM-2-4: Information Theoretic Security

Room 4 (Falcon)
Chair: Hiroki Koga (University of Tsukuba, Japan)

Post Encryption Compression with Affine Encoders for Secrecy Amplification in Distributed Source Encryption with Correlated Keys
Bagus Santoso (The University of Electro-Communications, Japan); Yasutada Oohama (University of Electro-Communications, Japan)
pp. 737-741

Distributed Hypothesis Testing with Privacy Constraints
Selma Belhadj Amor (BBM-Creative Media Works Pte, Singapore); Atefeh Gilani and Sadaf Salehkalaibar (University of Tehran, Iran); Vincent Y. F. Tan (National University of Singapore, Singapore)
pp. 742-746

A new proof of an inequality between two secrecy exponents
Ukyo Michiwaki and Yutaka Jitsumatsu (Kyushu University, Japan)
pp. 747-751