Book of Abstracts of

# 2020 International Symposium on Information Theory and its Applications

(ISITA2020)

**October 24 - 27, 2020**

**Sponsor**
Research Society of Information Theory and its Applications,
Engineering Sciences Society
IEICE

**Technical Co-Sponsor**
IEEE Information Theory Society

**Media Partner**
Entropy

**Financial Support**
Support Center for Advanced Telecommunications Technology Research Foundation
Kayanomori Foundation of Information Science Advancement
KIOXIA Corporation

Photo: Wikimedia Commons/Alakea1100 CC-BY 3.0

Book of Abstracts of

# 2020 International Symposium on Information Theory and its Applications

(ISITA2020)

# Welcome

## Message from the General Co-Chairs

It is our great pleasure and honor to welcome you to the 2020 International Symposium on Information Theory and its Applications, ISITA2020. The ISITA series of symposia was founded in 1990, and has been held every two years since then. The 2020 meeting is the sixteenth in the series, and the fifth one sponsored by the IEICE Research Society of Information Theory and its Applications, SITA. The original plan was for our symposium to be held in Hawaii, which is the birth-place of ISITA. As a challenge in the new normal, this year's ISITA2020 is run instead as a virtual conference.

We would like to express our deep gratitude to all the ISITA2020 Committee members for their hard work in making the symposium a great success. We are particularly grateful to the Technical Program Co-chairs, Professors Hiroshi Kamabe and Navin Kashyap, and all Technical Program Committee members for their extraordinary efforts in putting together and selecting an outstanding set of papers for the technical program. Our appreciation goes to Professors Olgica Milenkovic (University of Illinois at Urbana-Champaign), Masahito Hayashi (Southern University of Science and Technology/Nagoya University), and Paul H. Siegel (University of California San Diego) for being the plenary speakers.

Thank you all for your participation. We hope that you will have an enjoyable and rewarding experience at our virtual website.

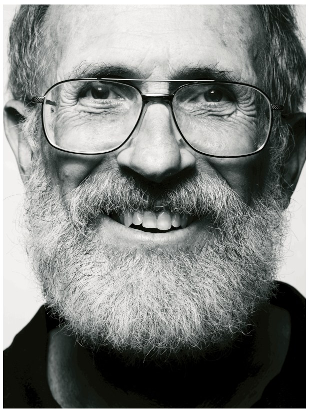
With Our ALOHA,

Manabu Hagiwara
Chiba University

James B. Nation
University of Hawaii

Ikuo Oka
Osaka City University

Prof. Manabu Hagiwara

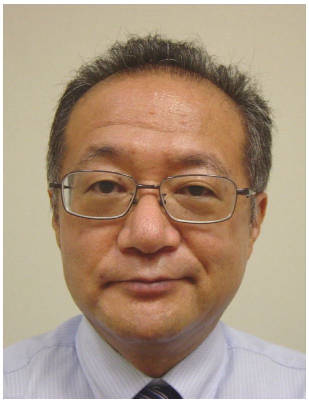


Prof. James B. Nation

Prof. Ikuo Oka

## Message from the Technical Program Committee Co-Chairs

Welcome to ISITA2020.



Prof. Hiroshi Kamabe

Prof. Navin Kashyap

Although we were unable to predict the form in which we would be able to conduct the event at the time of the submission deadline due to COVID-19, there were ultimately 160 submissions. Among the submissions, 124 were accepted. In July, it was decided that the submitted papers would be presented as on-demand videos.

We would like to thank our three eminent researchers Masahito Hayashi, Olgica Milenkovic, and Paul Siegel for accepting to present the plenary talks. These lectures will be released via live streaming. Furthermore, we would like to sincerely thank the authors for submitting their valuable research results, the reviewers for carefully reviewing them, and the members of the technical program committee for their wonderful work in deciding the acceptance/rejection of papers. We are extremely grateful to Yu Morishima for creating the technical program and processing the papers for publication. We would also like to extend our gratitude to the members of the organizing committee for their efforts in organizing the international conference in virtual format, which is unprecedented for ISITA, and for arranging the site for presentation.

Finally, we would like to thank Kenji Yasunaga, the Secretary of the Technical Program Committee, for his absolute dedication and efforts at all stages of the creation of the technical program, and for taking complete control of the two remote technical committee meetings spanning a total of over 12 hours and making it a success.

We look forward to enjoying ISITA 2020 with you over the Internet.

Hiroshi Kamabe
Gifu University

Navin Kashyap
Indian Institute of Science

# Symposium Committee

**General Co-Chairs**

Manabu Hagiwara (Chiba University)
James B. Nation (University of Hawaii)
Ikuo Oka (Osaka City University)

**Symposium Advisors**

Toru Fujiwara (Osaka University)
Anders Høst-Madsen (University of Hawaii)

**General Secretaries**

Shigeaki Kuzuoka (Wakayama University)
Hitoshi Tokushige (Kumamoto Gakuen University)
Hironori Uchikawa (KIOXIA Corporation)

**Finance**

Ryo Nomura (Waseda University)
Justin Kong (Kapiolani Community College)

**Publicity**

Brian M. Kurkoski (Japan Advanced Institute of Science and Technology)
Akiko Manada (Shonan Institute of Technology)

**Publications**

Yu Morishima (Tohoku Gakuin University)

**Registration**

Mitsugu Iwamoto (The University of Electro-Communications)

**Local Arrangement**

Takayuki Nozaki (Yamaguchi University)
Shoko Chisaki (Osaka Institute of Technology)

# Technical Program Committee

## Technical Program Committee Co-Chairs

Hiroshi Kamabe (Gifu University)
Navin Kashyap (Indian Institute of Science)

## Secretary

Kenji Yasunaga (Osaka University)

## TPC Members

Suayb S. Arslan (MEF University)
Kui Cai (Singapore University of Technology and Design)
Mao-Ching Chiu (National Chung Cheng University)
Elza Erkip (New York University)
Yuichiro Fujiwara (Chiba University)
Mitsuru Hamada (Tamagawa University Research Institute)
Masahito Hayashi (Nagoya University)
Masanori Hirotomo (Saga University)
Motohiko Isaka (Kwansei Gakuin University)
Koji Ishibashi (The University of Electro-Communications)
Ken-ichi Iwata (University of Fukui)
Sidharth Jaggi (Chinese University of Hong Kong)
Yuichi Kaji (Nagoya University)
Takafumi Kanamori (Tokyo Institute of Technology)
Kenta Kasai (Tokyo Institute of Technology)
Yutaka Kawai (Mitsubishi Electric Corporation)
Hiroki Koga (University of Tsukuba)
Tetsuya Kojima (National Institute of Technology, Tokyo College)
Gerhard Kramer (Technical University of Munich)
Noboru Kunihiro (University of Tsukuba)
Minoru Kuribayashi (Okayama University)
Brian M. Kurkoski (Japan Advanced Institute of Science and Technology)
Hidenori Kuwakado (Kansai University)
Akiko Manada (Shonan Institute of Technology)
Hajime Matsui (Toyota Technological Institute)
Ryutaroh Matsumoto (Nagoya University)
Ying Miao (University of Tsukuba)
Jun Muramatsu (NTT Corporation)
Toshihiro Niinomi (Tokyo City University)
Mikihiko Nishiara (Shinshu University)
Takashi Nishide (University of Tsukuba)
Yasuyuki Nogami (Okayama University)
Koji Nuida (The University of Tokyo)
Tomohiro Ogawa (The University of Electro-Communications)
Satoshi Takabe (Nagoya Institute of Technology)
Toyoo Takata (Iwate Prefectural University)
Junichi Takeuchi (Kyushu University)
Keigo Takeuchi (Toyohashi University of Technology)
Vincent Y. F. Tan (National University of Singapore)
Toshiyuki Tanaka (Kyoto University)

Van Khu Vu (Nanyang Technological University)
Tadashi Wadayama (Nagoya Institute of Technology)
Shun Watanabe (Tokyo University of Agriculture and Technology)
Eitan Yaakobi (Technion)
Hideki Yagi (The University of Electro-Communications)
Koji Yamamoto (Kyoto University)
Maki Yoshida (National Institute of Information and Communications Technology)

# International Advisory Committee

### International Advisory Committee Co-Chairs

Toshiyasu Matsushima (Waseda University)
Robert Morelos-Zaragoza (San Jose State University)

### IAC Members

Fady Alajaji (Queen's University)
Ezio Biglieri (Universitat Pompeu Fabra)
Richard E. Blahut (University of Pennslyvania)
Ning Cai (ShanghaiTech University)
Daniel Costello (University of Notre Dame)
Fang-Wei Fu (Nankai University)
Toru Fujiwara (Osaka University)
Anders Høst-Madsen (University of Hawaii)
Te Sun Han (National Institute of Information and Communications Technology)
Kees Immink (Turing Machines Inc.)
Gerhard Kramer (Technical University of Munich)
Mao-Chao Lin (National Taiwan University)
Shu Lin (University of California, Davis)
Hiroyoshi Morita (The University of Electro-Communications)
Prakash Narayan (University of Maryland)
Jong-Seon No (Seoul National University)
Yasutada Oohama (The University of Electro-Communications)
Masayoshi Ohashi (Fukuoka University)
Shlomo Shamai (Technion-Israel Institute of Technology)
Paul H. Siegel (University of California, San Diego)
Mikael Skoglund (KTH Royal Institute of Technology)
Ulrich Speidel (The University of Auckland)
A.J. Han Vinck (University of Duisburg-Essen)
Emanuele Viterbo (Monash University)
Branka Vucetic (The University of Sydney)
Jos H. Weber (Delft University of Technology)
Hirosuke Yamamoto (The University of Tokyo)
En-hui Yang (University of Waterloo)
Raymond W. Yeung (The Chinese University of Hong Kong)
Bin Yu (University of California, Berkeley)

# Sponsorship

**Sponsor**
Research Society of Information Theory and its Applications,
Engineering Sciences Society, IEICE

**Technical Co-Sponsor**
IEEE Information Theory Society

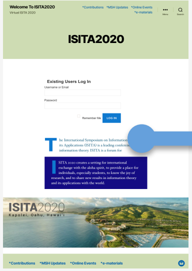
**Media Partner**
Entropy

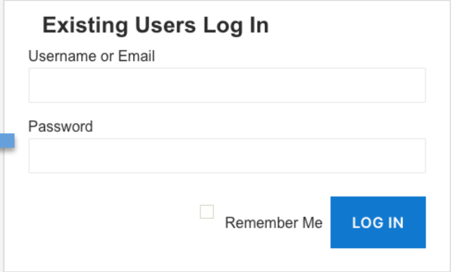
**Financial Support**
Support Center for Advanced Telecommunications Technology Research, Foundation
Kayamori Foundation of Informational Science Advancement
KIOXIA Corporation

# Getting Started with Virtual ISITA2020

## Log-in to the virtual site

- Visit the ISITA2020 virtual site at **https://isita.coresv.com/**.
- Enter username and password in the e-mail with subject line “Welcome to Virtual ISITA2020”, then click “LOG IN”.





### Existing Users Log In

Username or Email

Password

□ Remember Me

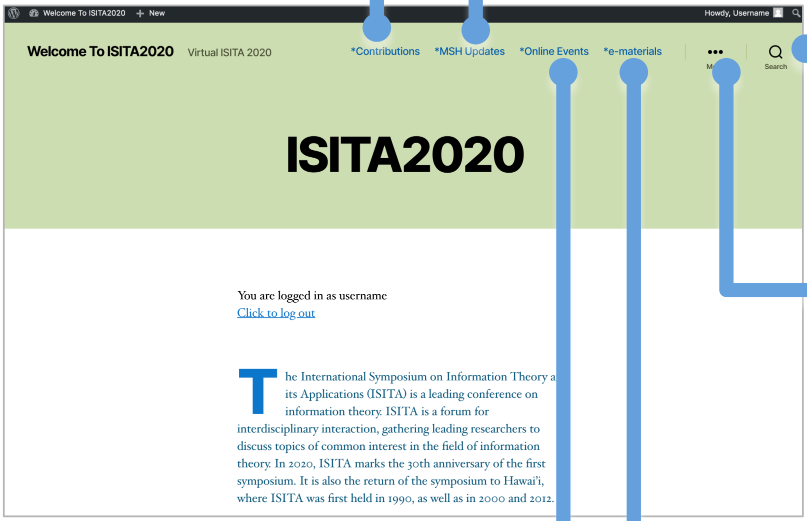
LOG IN

### Contributions

The first place to look for online presentations.

### MSH Updates (Must-See Hourly Updates)

Information will be announced hourly during the conference.



You are logged in as username

Click to log out

The International Symposium on Information Theory a its Applications (ISITA) is a leading conference on information theory. ISITA is a forum for interdisciplinary interaction, gathering leading researchers to discuss topics of common interest in the field of information theory. In 2020, ISITA marks the 30th anniversary of the first symposium. It is also the return of the symposium to Hawai'i, where ISITA was first held in 1990, as well as in 2000 and 2012.

### Search

Search for specific items.

### Menu

Click to show a quick access menu.

### Online Events

Click to check the events schedule and join the online events.

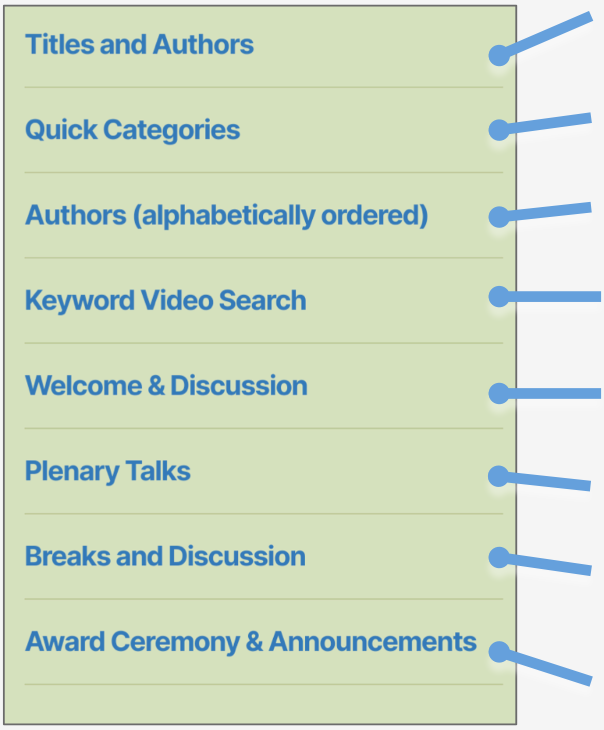
### e-materials

Book of Abstracts, conference proceedings and other materials are available.

* Online events will be held in Hawaii Time Zone (UTC -10).

# Menu

Click “menu” icon at the top right of the page to show the quick access menu.



Find contributions by title and authors.

Watch an introduction video of each category.

Find contributions by authors.

Find contributions by keyword.

Attend Welcome and discussion*.

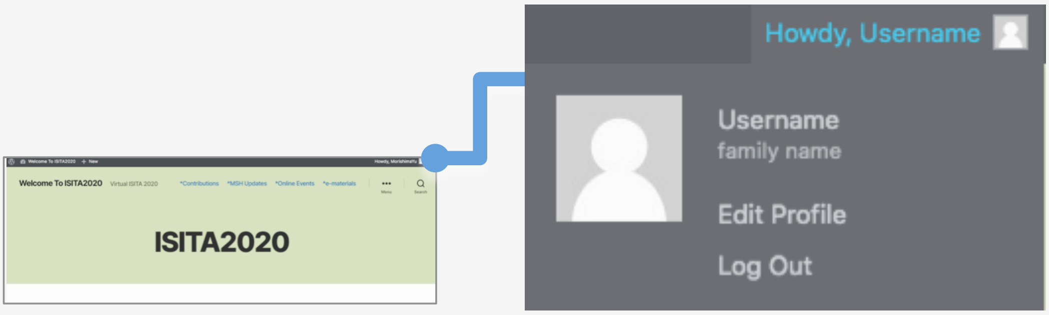
See information for plenary talks and attend plenary talk sessions*.

Attend breaks and discussion*.

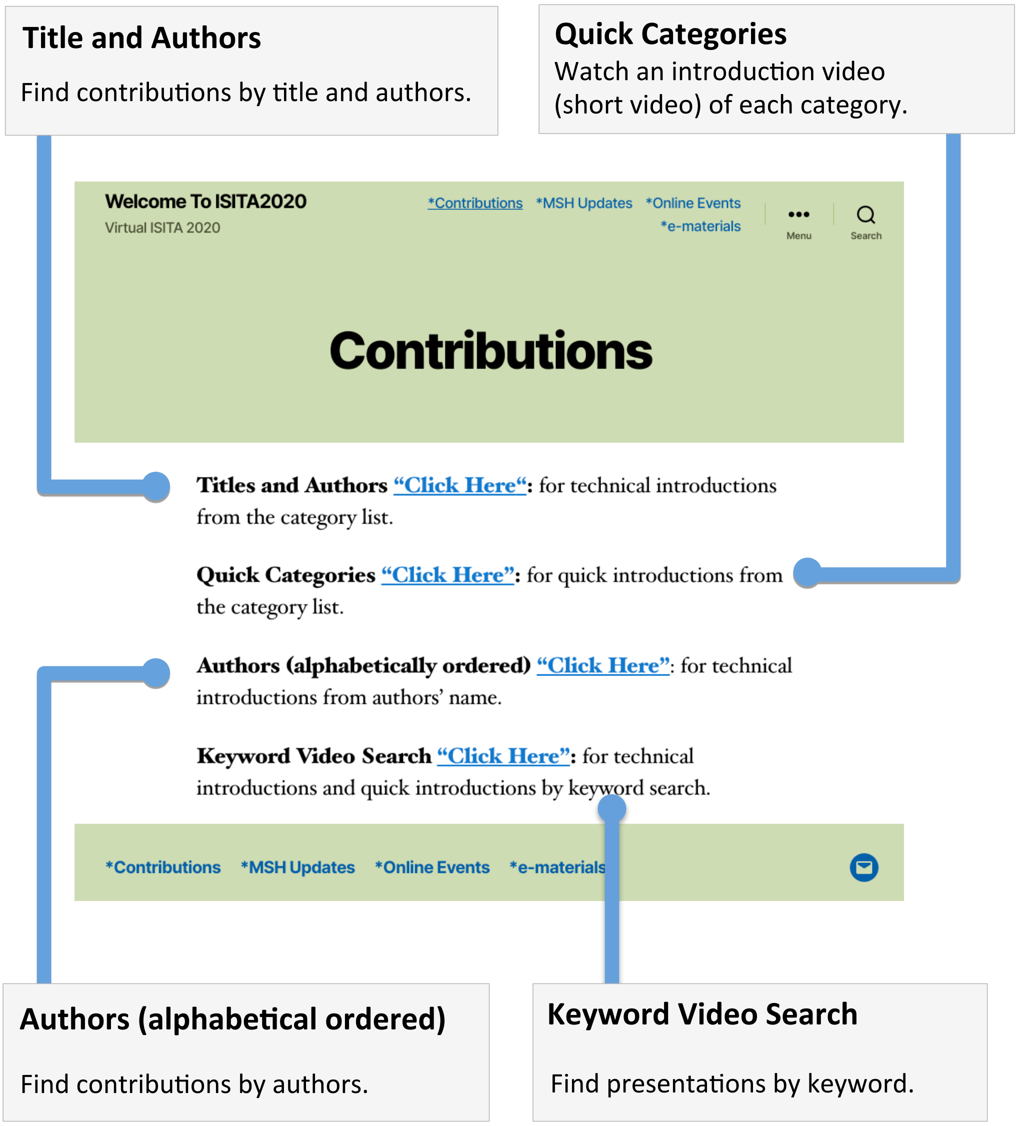
Attend award ceremony & announcements*.

# Personal Settings

- Click your username at the top right of the page to change your personal settings.
- In the option menu, you can change a color scheme, display name and other settings.



# Contributions



**Title and Authors**

Find contributions by title and authors.

**Quick Categories**

Watch an introduction video (short video) of each category.

## Contributions

**Titles and Authors "Click Here"**: for technical introductions from the category list.

**Quick Categories "Click Here"**: for quick introductions from the category list.

**Authors (alphabetically ordered) "Click Here"**: for technical introductions from authors' name.

**Keyword Video Search "Click Here"**: for technical introductions and quick introductions by keyword search.

**Authors (alphabetical ordered)**

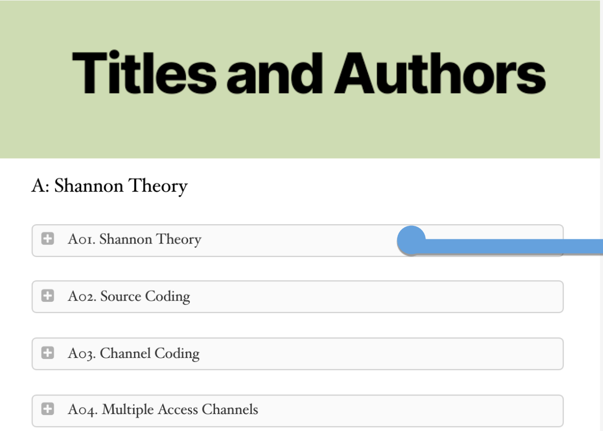
Find contributions by authors.

**Keyword Video Search**

Find presentations by keyword.

## Titles and Authors

- You can find presentations arranged by the category.
- To  expand a list of presentations, click the category menu.



# Titles and Authors

A: Shannon Theory

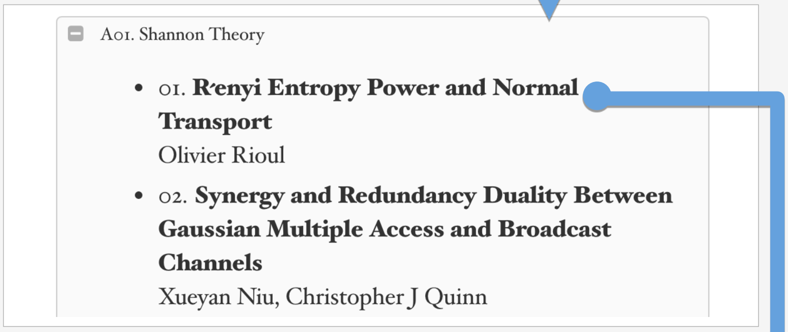
⊞ A01. Shannon Theory

⊞ A02. Source Coding

⊞ A03. Channel Coding

⊞ A04. Multiple Access Channels

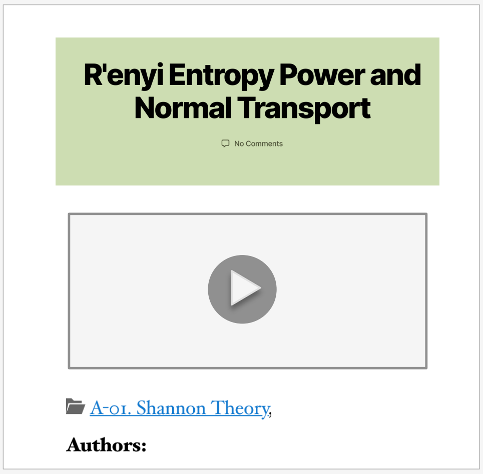
Click to expand a list.



⊟ A01. Shannon Theory

- 01. **R'enyi Entropy Power and Normal Transport**
Olivier Rioul
- 02. **Synergy and Redundancy Duality Between Gaussian Multiple Access and Broadcast Channels**
Xueyan Niu, Christopher J Quinn

Click to watch the  presentation.



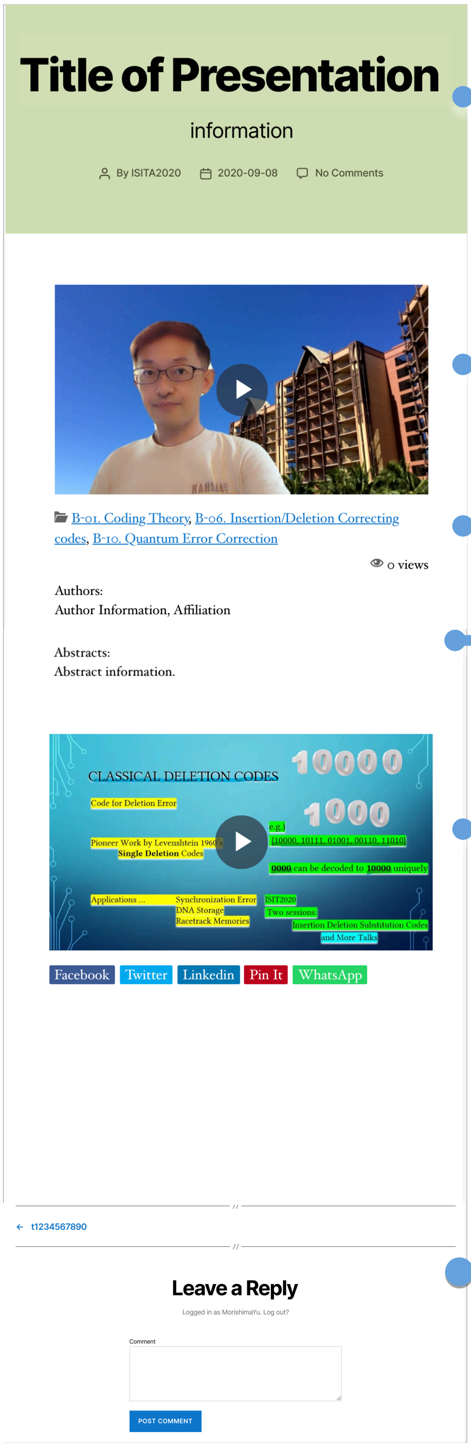
**R'enyi Entropy Power and Normal Transport**

No Comments

A-01. Shannon Theory,

**Authors:**

# Watch presentations



Title of Presentation

information

By ISITA2020 2020-09-08 No Comments

B-01. Coding Theory, B-06. Insertion/Deletion Correcting codes, B-10. Quantum Error Correction

0 views

Authors:
Author Information, Affiliation

Abstracts:
Abstract information.

Facebook Twitter Linkedin Pin It WhatsApp

← t1234567890

Leave a Reply

Logged in as MorishimaYu. Log out?

Comment

POST COMMENT

**Title of Presentation**

**Quick Introduction (short video)**

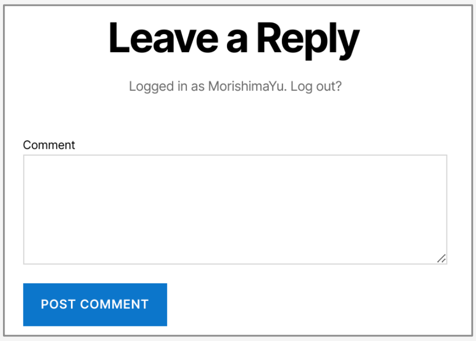
Find contributions by category tag.

**Author Information & Abstract**

**Technical Introduction (long video)**

**Leave a Reply**

You can post comments to presentations.



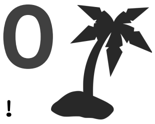
## Leave a Reply

Logged in as MorishimaYu. Log out?

Comment

POST COMMENT

# ACTION BINGO
# ISITA2020



Complete the challenges!

📅 Events

💬 Announcements

🗔 Virtual site features and materials

| | | | | |
|---|---|---|---|---|
| Participate in Welcome & Discussion 📅 | Check "MSH Updates" on Oct. 24th 💬 | Count the number of Call For Papers (in e-materials) 🗔 | Click "Online Events" from the menu bar 🗔 | Watch the Plenary Talk by Olgica Milenkovic 📅 |
| Use "Keyword Video Search" 🗔 | Download the e-Book of Abstracts from e-materials 🗔 | Join "Breaks and Discussions," Oct. 26th, 3pm-4pm 📅 | Make a new friend through "Breaks and Discussion" 📅 | Check "MSH Updates" on Oct. 25th 💬 |
| Check the dates and place for ISITA2022 💬 | Join the Award Ceremony & Announcements 📅 | Log-in to the virtual site 🗔 | Check the Sponsors on the front page 🗔 | Search the keyword "ISITA" from the "Search Icon" 🗔 |
| Check "MSH Updates" on Oct. 27th 💬 | Check if your acquaintances are giving presentations in "Authors (alphabetically ordered)" 🗔 | Join "Breaks and Discussion," Oct. 26th, 7pm-10pm 📅 | Watch two or more movies in "Quick Categories" 🗔 | Join "Breaks and Discussion," Oct. 27th, 7pm-10pm 📅 |
| . Watch the Plenary Talk by Masahito Hayashi 📅 | Change the color scheme from "Profile Menu" 🗔 | Leave your comments on three or more contributed presentations 🗔 | Check "MSH Updates" on Oct. 26th 💬 | Watch the Plenary Talk by Paul H. Siegel 📅 |

# Online Events

**Sunday, October 25 (HST, 14:00-17:00)** (UTC: Oct 26 0:00-3:00, JST: Oct 26 9:00-12:00)

14:00-17:00 **Welcome& Discussion (on Gather)**

**Monday, October 26 (HST, 14:00-22:00)** (UTC: Oct 27 0:00-8:00, JST: Oct 27 9:00-17:00)

14:00-15:00 **Plenary Talk 1 (on Zoom)**

**Semiquantitative Group Testing with Applications**
Prof. Olgica Milenkovic
*University of Illinois at Urbana-Champaign*

15:00-16:00 **Breaks & Discussion (on Gather)**

16:00-17:00 **Plenary Talk 2 (on Zoom)**

**Information-Theoretic Anonymous Cryptographic Protocols**
Prof. Masahito Hayashi
*Southern University of Science and Technology/Nagoya University*

19:00-22:00 **Breaks & Discussion (on Gather)**

**Tuesday, October 27 (HST, 14:00-22:00)** (UTC: Oct 28 0:00-8:00, JST: Oct 28 9:00-17:00)

14:00-15:00 **Plenary Talk 3 (on Zoom)**

**Costly Constrained Channels: Theory and Applications**
Prof. Paul H. Siegel
*University of California San Diego*

15:00-16:00 **Award Ceremony & Announcements (on Zoom)**

19:00-22:00 **Breaks & Discussion (on Gather)**

ISITA2020 will provide a venue for participants to interact with each other through Gather (*). More specifically, Welcome & Discussion and Breaks & Discussion. Welcome & Discussion will be held on October 25 from 2:00 pm to 5:00 pm (HST) to familiarize the participants with this forum. Breaks & Discussions will be held on October 26 from 3:00 pm to 4:00 pm and 7:00 pm to 10:00 pm, and October 27 from 7:00 pm to 10:00 pm (HST) in order to discuss the lectures with the presenters and among the participants.
There is also a space for you to have a chat, so please stop by.

For details, please refer to Online Events (**) of the conference website.

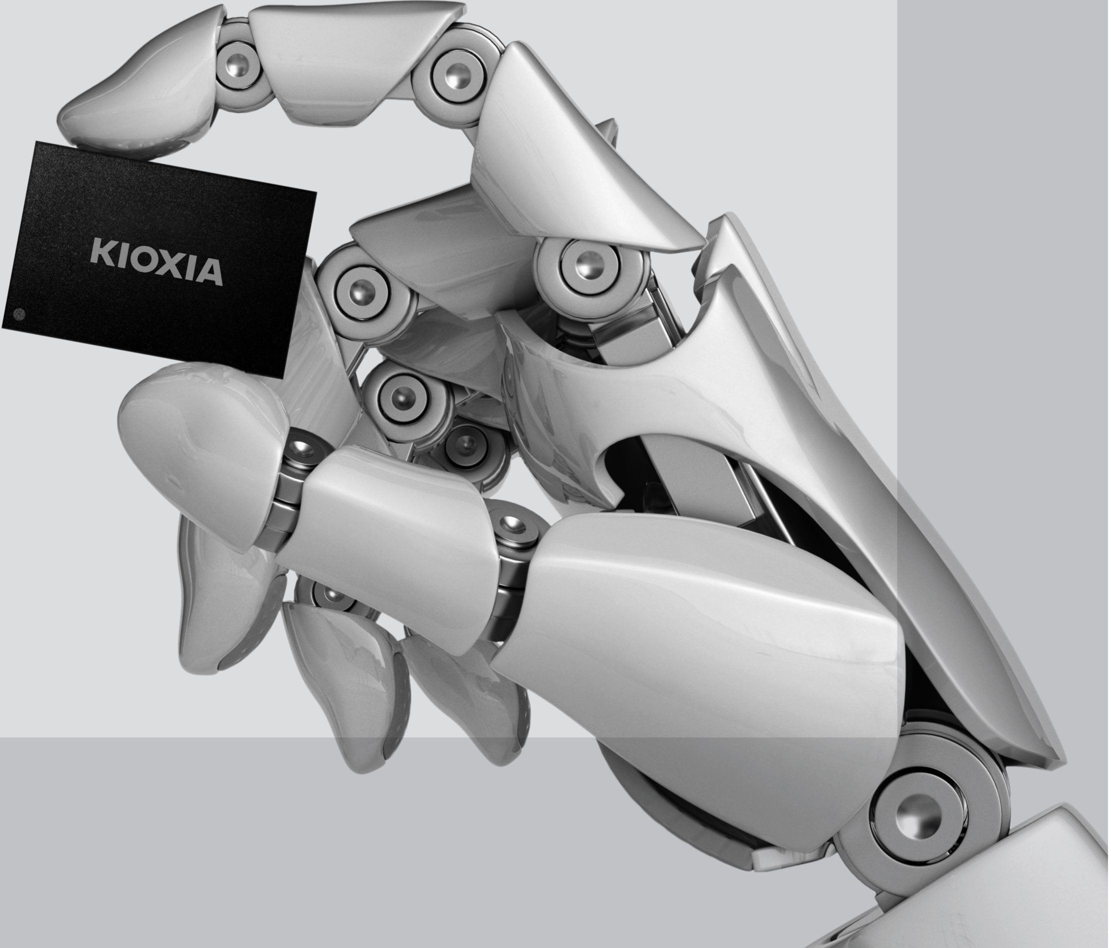
(*) https://gather.town/
(**) https://isita.coresv.com/online-events/

# Must-See Hourly Updates (MSH Updates)

Hourly updates regarding the symposium are displayed on the virtual symposium site. Please click on “MSH Updates” at the top of the site page and check the updates every day. This portal provides hourly useful information, including tips on how to use the site, tutorials on “Gather” for our online events, and greetings from the general co-chairs. To enjoy the full benefit of our symposium, please do not miss any updates. This will ensure the utmost clarity during the virtual symposium.

KIOXIA

# Uplifting the world with “memory”



# Category Index

2:00pm–3:00pm, October 26 (HST, UTC−10)
**Plenary Talk 1**

## Semiquantitative Group Testing with Applications

Prof. Olgica Milenkovic
*University of Illinois at Urbana-Champaign*

*Abstract:* Semiquantitative group testing (SQGT) is a group testing scheme motivated by a class of problems arising in genome screening experiments and testing for infectious diseases. SQGT may be viewed as a concatenation of an adder channel and an integer-valued quantizer and it represents a unifying framework for group testing and quantized compressive sensing. We will review the notions of SQ-disjunct and SQ-separable codes, and describe several combinatorial and probabilistic constructions for such codes. While for most of these constructions we assume that the number of defectives is significantly smaller than the total number of test subjects, we also consider the case for which there is no restriction on the number of defectives. We also review efficient decoding algorithms and describe an important application of this testing method for real time reverse-transcriptase polymerase chain reaction used as a gold standard for Covid-19 screening.

Prof. Olgica Milenkovic

*Biography:* Biography Olgica Milenkovic is a professor of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign (UIUC), and Research Professor at the Coordinated Science Laboratory. She obtained her Masters Degree in Mathematics in 2001 and PhD in Electrical Engineering in 2002, both from the University of Michigan, Ann Arbor. Prof. Milenkovic heads a group focused on addressing unique interdisciplinary research challenges spanning the areas of algorithm design and computing, bioinformatics, coding theory, machine learning and signal processing. Her scholarly contributions have been recognized by multiple awards, including the NSF Faculty Early Career Development (CAREER) Award, the DARPA Young Faculty Award, the Dean's Excellence in Research Award, and several best paper awards. In 2013, she was elected a UIUC Center for Advanced Study Associate and Willett Scholar while in 2015 she was elected a Distinguished Lecturer of the Information Theory Society. In 2018 she became an IEEE Fellow. She has served as Associate Editor of the IEEE Transactions of Communications, the IEEE Transactions on Signal Processing, the IEEE Transactions on Information Theory and the IEEE Transactions on Molecular, Biological and Multi-Scale Communications. In 2009, she was the Guest Editor in Chief of a special issue of the IEEE Transactions on Information Theory on Molecular Biology and Neuroscience.

4:00pm–5:00pm, October 26 (HST, UTC−10)
**Plenary Talk 2**

## Information-Theoretic Anonymous Cryptographic Protocols

Prof. Masahito Hayashi
*Southern University of Science and Technology/Nagoya University*

*Abstract:* In this talk, we present two information-theoretic cryptographic tasks related to anonymity and their protocols. One is secure list decoding and the other is multi-party anonymous unanimous approval.

Secure list decoding is an extended task of list decoding by adding security requirements. While the conventional list decoding requires that the list contains the transmitted message, secure list decoding requires the following additional security conditions. The first additional security condition is the impossibility of the correct decoding, i.e., the receiver cannot uniquely identify the transmitted message even though the transmitted message is contained in the list. This condition can be trivially satisfied when the transmission rate is larger than the channel capacity. The other additional security condition is the impossibility for the sender to estimate another element of the decoded list except for the transmitted message. This protocol can be used for anonymous auction, which realizes the anonymity for bidding. We characterize the asymptotic achievable rate region for this task when these requirements are required information-theoretically.

Multi-party anonymous unanimous approval is a task when a certain project written as the variable $Y \in F_q^d$ requires the approvals from all of m players. Our requirements are the following. We verify that all m players approve the project by confirming the contents $Y$. Also, the correctness of distributed contents among the m players needed to be verified. When a player disagrees, the player cannot be identified. This task can be realized information-theoretically by using secure modulo summation, which is a new cryptographic resource.

A part of the presented results is a joint work with Takeshi Koshiba.
Proc. ISIT2019, pp. 1727 – 1731; https://arxiv.org/abs/1901.02590 ;
https://arxiv.org/abs/1910.05976 ; https://arxiv.org/abs/1812.10862 ;
https://eprint.iacr.org/2018/802.pdf

Prof. Masahito Hayashi

*Biography:* Masahito Hayashi received the B.S. degree from the Faculty of Sciences in Kyoto University, Japan, in 1994 and the M.S. and Ph.D. degrees in Mathematics from Kyoto University, Japan, in 1996 and 1999, respectively. He worked in Kyoto University as a Research Fellow of the Japan Society of the Promotion of Science (JSPS) from 1998 to 2000, and worked in the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN from 2000 to 2003, and worked in ERATO Quantum Computation and Information Project, Japan Science and Technology Agency (JST) as the Research Head from 2000 to 2006. He worked in the Graduate School of Information Sciences, Tohoku University as Associate Professor from 2007 to 2012. In 2012, he joined the Graduate School of Mathematics, Nagoya University as Professor. In 2020, he joined Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China as Chief Research Scientist. In 2011, he received Information Theory Society Paper Award (2011) for “Information-Spectrum Approach to Second-Order Coding Rate in Channel Coding”. In 2016, he received the Japan Academy Medal from the Japan Academy and the JSPS Prize from Japan Society for the Promotion of Science. In 2017, he was promoted to IEEE Fellow.

In 2006, he published the book “Quantum Information: An Introduction” from Springer, whose revised version was published as “Quantum Information Theory: Mathematical Foundation” from Graduate Texts in Physics, Springer in 2016. In 2016, he published other two books “Group Representation for Quantum Theory” and “A Group Theoretic Approach to Quantum Information” from Springer. His research interests include classical and quantum information theory and classical and quantum statistical inference.

2:00pm–3:00pm, October 27 (HST, UTC−10)
**Plenary Talk 3**

## Costly Constrained Channels: Theory and Applications

Prof. Paul H. Siegel
*University of California San Diego*

*Abstract:* Finite-state noiseless channels with symbol costs − or, costly constrained channels − trace their origins to Shannon's analysis of the telegraph channel in 1948. They serve as useful models in many data transmission, storage, and networking scenarios. The study of their information-theoretic properties has fascinating intersections with analytical combinatorics, matrix analysis, optimization theory, and the theory of finite-state Markov chains. A variety of algorithmic approaches to designing efficient codes have been proposed, drawing on enumerative methods, source coding, symbolic dynamics, and tree coding. In this talk, I will present two recent problems in information storage that can be formulated in terms of costly constrained channels: rate-constrained data shaping to extend the lifetime of flash memory, and coding for efficient strand synthesis in DNA-based data storage. I will discuss theoretical results and coding schemes, both old and new, that have been used to address them, highlighting several of the interesting connections mentioned above.

Prof. Paul H. Siegel

*Biography:* Paul Siegel is a Distinguished Professor of Electrical and Computer Engineering in the Jacobs School of Engineering at the University of California San Diego, where he holds an endowed chair at the Center for Memory and Recording Research. He received undergraduate and graduate degrees in mathematics from the Massachusetts Institute of Technology in 1975 and 1979, respectively. He held a Chaim Weizmann Postdoctoral Fellowship with the Courant Institute at New York University. He was with the IBM Research Division in San Jose, California from 1980 to 1995, and joined the faculty at UC San Diego in 1995. Prof. Siegel has been working on applications of information theory and coding to problems in data storage for 40 years. He was co-recipient of the 1992 IEEE Information Theory Society Paper Award and the 1993 IEEE Communications Society Leonard G. Abraham Prize Paper Award in recognition of his work in this area. He was also co-recipient of the 2007 Best Paper Award in Signal Processing and Coding for Data Storage from the Data Storage Technical Committee of the IEEE Communications Society. He was the Padovani Lecturer of the IEEE Information Theory Society in 2015. He is an IEEE Fellow and a member of the U.S. National Academy of Engineering. Prof. Siegel was a Member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and from 2009 to 2014. He served the IEEE Transactions on Information Theory as Co-Guest Editor of the 1991 Special Issue on Coding for Storage Devices, Associate Editor of Coding Techniques from 1992 to 1995, and Editor-in-Chief from 2001 to 2004. He also served the IEEE Journal on Selected Areas in Communications as Co-Guest Editor of the 2001 two-part issue on The Turbo Principle: From Theory to Practice and the 2016 issue on Recent Advances in Capacity Approaching Codes.

## Shannon Theory

A01-01

### Rényi Entropy Power and Normal Transport

*Olivier Rioul*

A framework for deriving Rényi entropy-power inequalities (REPIs) is presented that uses linearization and an inequality of Dembo, Cover, and Thomas. Simple arguments are given to recover the previously known Rényi EPIs and derive new ones, by unifying a multiplicative form with constant c and a modification with exponent $\alpha$ of previous works. An information-theoretic proof of the Dembo-Cover-Thomas inequality—equivalent to Young's convolutional inequality with optimal constants—is provided, based on properties of Rényi conditional and relative entropies and using transportation arguments from Gaussian densities. For log-concave densities, a transportation proof of a sharp varentropy bound is presented.

A01-02

### Synergy and Redundancy Duality Between Gaussian Multiple Access and Broadcast Channels

*Xueyan Niu, Christopher J Quinn*

We investigate a novel duality for scalar Gaussian multiple access channels and broadcast channels. The duality we explore is based on shared partial information quantities (e.g. synergy and redundancy). Using lattice theory, we establish a crossover correspondence of the synergistic and redundant components between these two channels. The dual channels are similar to the traditional pairs based on capacity regions, though the pairs we identify have equal transmission powers instead of a sum constraint relating transmission powers.

A01-03

### On the Capacity of the Flash Memory Channel with Feedback

*V. Arvind Rameshwar, Aryabhatt M. Reghu, Navin Kashyap*

In this paper, the binary channel that changes the 101 input pattern to a 111 with probability $\epsilon$, and leaves the other input patterns unchanged, is considered as a model for inter-cell interference (ICI) in NAND flash memories. The capacity with feedback of this channel is cast as a dynamic programming (DP) problem, and is numerically evaluated using the value iteration procedure. An analytical upper bound on the feedback capacity is derived using the "$Q$-graph"-based technique of Sabag et al., and the bound is shown to be numerically close in value to the feedback capacity arrived at from the DP problem. For the special case of the channel where $\epsilon$ is equal to 1 (which we call the deterministic flash memory channel), the capacities with and without feedback (which are identical) are shown to be roughly 0.8114, which, in turn, is the capacity of the constrained system that forbids the 101 input pattern.

A01-04

### On Two Information Quantities Relating Two Distortion Balls

*Shota Saito, Toshiyasu Matsushima*

This paper clarifies the relationship between two information quantities related to two distortion balls in variable-length lossy source coding. To show various fundamental limits in variable-length lossy source coding, the notion of distortion ball has been known to be useful. In the previous study by Kostina et al., it was shown that the fundamental limit of the minimum average codeword lengths under an excess distortion constraint is characterized by the information quantity related to the distortion ball centered at a source symbol. On the other hand, in our previous study, it was shown that the same fundamental limit is characterized by the information quantity related to the distortion ball centered at a reproduction symbol. Then, what is the relationship between these two information quantities? This paper gives an answer to this question.

A01-05

### An Equivalent Expression for the Wyner-Ziv Source Coding Problem

*Tetsunao Matsuta, Tomohiko Uyematsu*

We consider the coding problem for lossy source coding with side information at the decoder, which is known as the Wyner-Ziv source coding problem. The goal of the coding problem is to find the minimum rate such that the probability of exceeding a given distortion threshold is less than the desired level. We give an equivalent expression of the minimum rate by using the chromatic number and a notion of covering of a set. This allows us to analyze the coding problem in terms of graph coloring and covering.

A01-06

### A Study on the Overflow Probability of Variable-to-Fixed Length Codes

*Shigeaki Kuzuoka*

The overflow probability (i.e., the probability that the empirical compression rate exceeds a given threshold) of variable-to-fixed length codes is studied. Particularly, (i) the optimum threshold such that the overflow probability is asymptotically bounded by a given constant, and (ii) the optimum exponent of the overflow probability for a given threshold are investigated.

A01-07

### Remote Empirical Coordination

*Michail Mylonakis, Photios A. Stavrou, Mikael Skoglund*

We apply the framework of imperfect empirical coordination to a two-node setup where the action $X$ of the first node is not observed directly but via $L$ agents who observe independently impaired measurements $\hat{X}$ of the action. These $L$ agents, using a rate-limited communication that is available to all of them, help the second node to generate the action $Y$ in order to establish the desired coordinated behaviour. When $L < \infty$, we prove that it suffices $R_i \geq I\left(\hat{X};\hat{Y}\right)$ for at least one agent whereas for $L \longrightarrow \infty$, we show that it suffices $R_i \geq I\left(\hat{X};\hat{Y}|X\right)$ for all agents where $\hat{Y}$ is a random variable such that $X - \hat{X} - \hat{Y}$ and $\|p_{X,\hat{Y}}\left(x,y\right) - p_{X,Y}\left(x,y\right)\|_{TV} \leq \Delta$ ( $\Delta$ is the pre-specified fidelity).

A01-08

### Exponent Function for the Gel'fand-Pinsker Channel at Rates above the Capacity

*Yasutada Oohama*

We consider the state dependent channels with full state information with at the sender. For this state dependent channel, the channel capacity was determined by Gel'fand and Pinsker. In this paper, we study the correct probability of decoding at rates above the capacity. We prove that when the transmission rate is above the capacity this probability goes to zero exponentially and derive an explicit lower bound of this exponent function.

A01-09

### Entropy to Control Planning in Video-Games

*Eric Jacopin*

We consider the problem of controlling the online planning of the behaviors of non-player characters (NPCs) in video-games. We present an urn model of this online planning of the behaviors of NPCs where urns are NPCs, the plans correspond to balls in an urn, and the type of a plan correspond to the color of a ball, to compute the information entropy of the planning activity. We compare this model with the planning entropy measurements from six commercial First-Person Shooters: our model predicts successive variations in entropy and sometimes closely adjusts to experimental values; we thus provide macroscopic parameters and combine them in a simple ratio to control the planning of behaviors of NPCs.

A01-10

### Trellis Code Error Exponent From Results for Asynchronous Multiple Access Channels

*Lóránt Farkas*

An asynchronous multiple access error exponent result implicates a new result for time invariant trellis codes of memory 1.

A01-11

### Minimum Energy Analysis for Robust Gaussian Joint Source-Channel Coding with a Square-Law Profile

*Mohammadamin Baniasadi, Ertem Tuncel*

A distortion-noise profile is a function indicating the maximum allowed source distortion value for each noise level in the channel. In this paper, the minimum energy required to achieve a distortion noise profile is studied for Gaussian sources transmitted over Gaussian channels. Previously known lower and upper bounds for the minimum required energy to achieve the square-law profile are improved using a family of lower bounds and our proposed coding scheme.

A01-12

### On Berger-Tung Inner Bound for Sum-Rate versus Sum-Distortion Problem

*Srinivas Avasarala, Sharang Sriram, Soumya Jana*

While tightness of the Berger-Tung inner bound has been established in the quadratic Gaussian case, and its slackness has been demonstrated in another case dealing with sources with common information, the underlying tightness/slackness issue remains to be settled in several scenarios. In this context, seeking to study a simple variant of the Berger-Tung problem, we consider doubly symmetric binary sources, Hamming distortion measures, and sum-rate versus sum-distortion. As a first step, in this paper we propose two functions admitting closed-form expressions, prove their local optimality in certain sense, conjecture that those functions specify the Berger-Tung inner bound, and present simulation-based evidence in support of such conjecture.

A01-13

### Coding Theorems on the Simple Capacity for Digital Fingerprinting Codes

*Hiroki Koga*

Digital fingerprinting codes provide a method to protect licensed digital contents against illegal redistribution. We focus on the situation where two malicious users collude and generate an overwritten codeword by using a memoryless collusion channel. We investigate coding theorems for the digital fingerprinting codes using a simple decoder such that each user is judged as malicious or innocent from an overwritten codeword together with his/her codeword. We first discuss the case where the collusion channel is known. We give a formula of the simple capacity. Next, we consider the case where the collusion channel is unknown. We succeed in giving the formula of a simple capacity of this case as well.

## Source Coding

A02-01

### Gauss-Markov Source Tracking with Side Information: Lower Bounds

*Omri Lev, Anatoly Khina*

We consider the problem of causal source coding and causal decoding of a Gauss-Markov source, where the decoder has causal access to a side-information signal. We define the information causal rate-distortion function with causal decoder side information and prove that it bounds from below its operational counterpart. We further explain how to adapt the result to the setting of control over communication channels.

A02-02

### Address-Event Variable-Length Compression for Time-Encoded Data

*Sharu Theresa Jose, Osvaldo Simeone*

Time-encoded signals, such as social network update logs and spiking traces in neuromorphic processors, are defined by multiple traces carrying information in the timing of events, or spikes. When time-encoded data is processed at a remote site with respect to the location in which it is produced, the occurrence of events needs to be encoded and transmitted in a timely fashion. The standard Address-Event Representation (AER) protocol for neuromorphic chips encodes the indices of the "spiking" traces in the payload of a packet produced at the same time the events are recorded. This implicitly encodes the events' timing in the timing of the packet (which is assumed to be correctly detected at the receiver). This paper investigates the potential bandwidth saving that can be obtained by carrying out variable-length compression of packets' payloads. Compression leverages both intra-trace and inter-trace correlations over time that are typical in applications such as social networks or neuromorphic computing. The approach is based on discrete-time Hawkes processes and entropy coding with conditional codebooks. Results from an experiment based on a real-world retweet dataset are also provided.

A02-03

### Third-Order Asymptotics of Variable-Length Compression Allowing Errors

*Yuta Sakai, Vincent Y. F. Tan*

This study investigates the fundamental limits of variable-length compression in which prefix-free constraints are not imposed (i.e., one-to-one codes are studied) and non-vanishing error probabilities are permitted. Due in part to a crucial relation between the variable-length and fixed-length compression problems, our analysis requires a careful and refined analysis of the fundamental limits of fixed-length compression in the setting where the error probabilities are allowed to approach either zero or one polynomially in the blocklength. To obtain the refinements, we employ tools from moderate deviations and strong large deviations. Finally, we provide the third-order asymptotics for the problem of variable-length compression with non-vanishing error probabilities. We show that unlike several other information-theoretic problems in which the third-order asymptotics are known, for the problem of interest here, the third-order term depends on the permissible error probability.

A02-04

### Autoregressive Image Generative Models with Normal and t-distributed Noise and the Bayes Codes for Them

*Yuta Nakahara, Toshiyasu Matsushima*

In this paper, we propose an autoregressive stochastic generative model for images. This model should be one of the most basic models for the new type of lossless image compression which explicitly assume the stochastic generative model. We can easily expand it and theoretically interpret the implicitly assumed stochastic generative models in the various previous predictive coding methods as the expanded versions of our model. Moreover, we can utilize the achievements in the related fields where the linear regression analysis and its expansion are studied to construct the Bayes codes for these generative models. As an example, we expand our generative model from the one with normal noise to the one with the t-distributed noise. Then, we construct the sub-optimal Bayes codes for this generative model by utilizing the variational Bayesian method.

## Channel Coding

A03-01

### An Effective Learning Scheme for Weighted-BP with Parallel Permutation Decoding

*Ryota Yoshizawa, Kenichiro Furuta, Yuma Yoshinaga, Osamu Torii, Tomoya Kodama*

Weighted-BP is a method to improve the decoding performance of belief-propagation (BP) by learning its appropriate message weights using deep learning technique. For binary primitive BCH codes, it has been reported in literature that their performance can be enhanced more through parallel decoding which is achieved by exploiting the automorphism property of the codes. In this paper, an effective learning scheme for the parallel weighted-BP is proposed. While in the conventional work the weights preliminarily learned for a single weighted-BP were utilized as is even in the scenario of parallel decoding, we show that some gain can be further obtained if we take the parallel structure into account in the learning phase.

A03-02

### Maximum Likelihood Channel Decoding with Quantum Annealing Machine

*Naoki Ide, Tetsuya Asayama, Hiroshi Ueno, Masayuki Ohzeki*

We formulate maximum likelihood (ML) channel decoding as a quadratic unconstraint binary optimization (QUBO) and simulate the decoding by the current commercial quantum annealing machine, D-Wave 2000Q. We prepared two implementations with Ising model formulations, generated from the generator matrix and the parity-check matrix respectively. We evaluated these implementations of ML decoding for low-density parity-check (LDPC) codes, analyzing the number of spins and connections and comparing the decoding performance with belief propagation (BP) decoding and brute-force ML decoding with classical computers. The results show that these implementations are superior to BP decoding in relatively short length codes, and while the performance in the long length codes deteriorates, the implementation from the parity-check matrix formulation still works up to 1k length with fewer spins and connections than that of the generator matrix formulation due to the sparseness of parity-check matrices of LDPC.

A03-03

### Orthogonal Sparse Superposition Codes

*Yunseo Nam, SongNam Hong, Namyoon Lee*

This paper presents a new class of sparse superposition codes for efficient short-packet and low-rate communication over the AWGN channel. The new codes are orthogonal sparse superposition (OSS) codes, in which a codeword is constructed by a superposition of orthogonal columns of a dictionary matrix. We propose a successive encoding technique to construct such codewords. In addition, we introduce a near-optimal decoding, named an element-wise maximum a posterior decoding with successive support set cancellation, which has a linear decoding complexity in block lengths. Via simulations, we demonstrate that the proposed encoding and decoding techniques are less complex and better performing than existing coded modulation techniques for reliable short packet communications.

A03-04

### Codes for high-noise memoryless channels

*Ilya Dumer, Navid Gharavi*

We consider code design for high-noise memoryless channels, which emerge in various low-power applications, such as IoT or sensor networks. To address this case, we design simple LDPC-type codes that have growing dimension m and length $m(m+1)/2$. These codes can be regarded as a ”weakly-coded” modulation: they outperform uncoded modulation for the signal-to-noise ratios (SNR) above -3 dB per information bit and achieve a 3 dB gain as SNR grows. Similar to uncoded modulation, these codes also exhibit a floor on the output bit error rate (BER) for any $m$. To improve code performance, information bits are further protected with some polar code of length $m$. The overall design has low complexity of order $m^2 \log m$ and a vanishing BER of order $\exp\{-m^{1/2}\}$. It substantially outperforms biorthogonal codes for any $SNR > 0$ dB given the same code rate or blocklength.

## Quantum Information Theory

A06-01

### Effect of Non-Gaussian Noise Due to Beam Wandering on Error Performance of Quantum Measurement

*Tiancheng Wang, Tsuyoshi Usuda*

In the efforts to apply quantum communication to atmospheric channels and on an intercontinental scale, a diverse range of inherent effects in the quantum channel have been attracting research attention in recent years. Beam wandering is an inherent effect that is known to occur when wireless communication methods such as satellite-based global communications are considered, and a previous study on these terms provides a good example of non-Gaussian noise. In our study, we present and consider the error performances for optimum quantum measurement, suboptimal measurement, and optimum classical measurement approaches using an $M$-ary phase-shift keying modulation scheme when beam wandering occurs.

A06-02

### Performance Evaluation of Ghost Imaging with Orthogonal/Non-orthogonal Quantum States in Terms of Image Quality

*Yuto Takahashi, Tiancheng Wang, Shogo Usami, Tsuyoshi Usuda*

Entangled states constructed from non-orthogonal quantum states have outperformed those constructed from orthogonal states for several application protocols. Nevertheless, the performances achieved with these states depend on the application protocol. With regard to non-orthogonal states, the performance of quantum ghost imaging has not been considered. Quantum ghost imaging is an imaging technique that exploits entangled states. In our previous works, we revealed that the error probability of the ghost imaging with non-orthogonal states can be better than that with orthogonal states in some cases. In this work, we compare the visibility performance of quantum ghost imaging when using orthogonal quantum states and non-orthogonal quantum states.

A06-03

### Quantum Illumination using Quasi-Bell States

*Jun Yamauchi, Yuto Takahashi, Tiancheng Wang, Tsuyoshi Usuda*

Quantum illumination is one of the application protocols of entanglement. This protocol uses entanglement for target detection. The protocol was first proposed by Lloyd, and its performance was later studied by Tan et al. In a lossy environment, they considered a Gaussian state in the presence of thermal noise. Entanglement with nonorthogonal states, such as coherent states, produces “quasi-Bell states.” These states have been shown to be capable of “perfect entanglement.” In this paper, we consider quantum illumination using quasi-Bell states, and compute the minimum error probability of quantum illumination under these states.

A06-04

### Simplification of the Calculation of the Channel Matrix for AMPM Coherent-state Signals

*Ryusuke Miyazaki, Mana Yoshida, Tiancheng Wang, Tsuyoshi Usuda*

The square-root measurement (SRM) is regarded as the optimum quantum measurement for symmetric signals and quasi-optimum measurements for any quantum signals. Therefore, deriving formulae for the channel matrix by using SRM is crucial in developing a theory of quantum communications. To date, formulae for these matrices are known for symmetric and group-covariant signals. However, there are important non-symmetric signals such as ASK, AMPM, and QAM signals, etc. In this paper, we demonstrate that the calculation of the channel matrix for $4m$-ary AMPM signals can be simplified by using their partial symmetry.

## Coding Theory

B01-01

### Design of ZDF code using uniform shift enumerator

*Yuya Naruse, Shan Lu, Hiroshi Kamabe*

The fountain code is an erasure correcting code used for the packet erasure channel. ZDF codes (Zigzag Decodable Fountain codes) are a kind of fountain codes which are generalizations of Raptor codes. The distinguishing characteristic of ZDF codes is to apply bit shift operation to generate the encoded packets. The bit-wise peeling decoding (PA) is used based on the difference bit shift of the precoded packets to the encoded packets. To provide more start of bit-wise PA, we investigate the enumerator of the encoded packets' shift combinations. We found that the shift combination of all the degree of the encoded packet has the uniform enumerator, the packets can have an effective start for bit-wise PA. Thus, we propose a ZDF code with variable shift distribution based on shift combinations with a uniform enumerator. From the simulation results, we have shown that the decoding erasure rate per received packet is decreased compared with other methods by limiting the number of selection of each shift and suppressing the deviation of the shifts.

B01-02

### A family of perfectness of the Levenshtein codes $\mathrm{L}_a(n;2n)$

*Kento Nakada*

The author introduces a family of new classes of double deletion errors, what he calls double deletion errors of type $\sigma$, and prove that the Levenshtein codes $L_a(n;2n)$ are perfect under double deletion errors of type $\sigma$.

B01-03

### Theoretical Estimates of Burst Error Probability for Convolutional Codes

*Anastasiia Smeshko, Fedor Ivanov, Victor V. Zyablov*

In this paper, we consider burst distribution at the output of Viterbi decoder for the binary symmetric channel. We suggest a new approach for the burst error probability evaluation based on active distances for the convolutional code. Using distance properties we also define a spectrum of active distances to analyze code performance. We obtain the expressions for lower and upper bounds on the burst error probability. These expressions are based on active distances and on their distance spectrum. In this paper, we consider convolutional codes with recursive encoder and rate one half.

B01-04

### Coded Computing for Boolean Functions

*Chien-Sheng Yang, Salman Avestimehr*

The growing size of modern datasets necessitates splitting a large scale computation into smaller computations and operate in a distributed manner for improving overall performance. However, adversarial servers in a distributed computing system deliberately send erroneous data in order to affect the computation for their benefit. Computing Boolean functions is the key component of many applications of interest, e.g., classification problem, verification functions in the blockchain and the design of cryptographic algorithm. In this paper, we consider the problem of computing a Boolean function in which the computation is carried out distributively across several workers with particular focus on security against Byzantine workers. We note that any Boolean function can be modeled as a multivariate polynomial which can have high degree in general. Hence, the recently proposed Lagrange Coded Computing (LCC) can be used to simultaneously provide resiliency, security, and privacy. However, the security threshold (i.e., the maximum number of adversarial workers that can be tolerated) provided by LCC can be extremely low if the degree of the polynomial is high. Our goal is to design an efficient coding scheme which achieves the optimal security threshold. We propose two novel schemes called coded Algebraic normal form (ANF) and coded Disjunctive normal form (DNF). Instead of modeling the

Boolean function as a general polynomial, the key idea of the proposed schemes is to model it as the concatenation of some linear functions and threshold functions. The proposed coded ANF and coded DNF outperform LCC by providing the security threshold which is independent of the polynomial's degree.

B01-05

### On Optimal Finite-length Binary Codes of Four Codewords for Binary Symmetric Channels

*Yanyan Dong, Shenghao Yang*

Finite-length binary codes of four codewords are studied for memoryless binary symmetric channels (BSCs) with the maximum likelihood decoding. For any block-length, best linear codes of four codewords have been explicitly characterized, but whether linear codes are better than nonlinear codes or not is unknown in general. In this paper, we show that for any block-length, there exists an optimal code of four codewords that is either linear or in a subset of nonlinear codes, called Class-I codes. Based on the analysis of Class-I codes, we derive sufficient conditions such that linear codes are optimal. For block-length less than or equal to 8, our analytical results show that linear codes are optimal. For block-length up to 300, numerical evaluations show that linear codes are optimal.

B01-06

### Upper Bounds on the Error Probability for the Ensemble of Linear Block Codes with Mismatched Decoding

*Toshihiro Niinomi, Hideki Yagi, Shigeichi Hirasawa*

In this paper, applying the technique of the DS2 bound, we derive an upper bound on the error probability of mismatched decoding with the ensemble of linear block codes, which was defined by Hof, Sason and Shamai. Assuming the ensemble of random linear block codes defined by Gallager, we show that the obtained bound is not looser than the conventional bound.

B01-07

### Property of Quantum Decoding for Sourlas Codes of Which Tuples Are Randomly Decimated

*Sangook Lee, Kazunori Iwata, Kazushi Mimura*

We propose the decimated Sourlas codes, which is an analogue of the Sourlas codes. In the decimated Sourlas codes, tuples are randomly decimated to control the code rate. We analyse its quantum decoding property using a statistical mechanical method and show that the bit error rate can be controlled.

B01-08

### Upper and Lower Estimates of Frame Error Rate for Convolutional Codes

*Anastasiia Smeshko, Fedor Ivanov, Victor V. Zyablov*

In this paper, we suggest a new approach for frame error rate (FER) evaluation for the convolutional codes. We consider binary symmetric channel and Viterbi decoding of convolutional codes. Convolutional codes we studied here have code rate one half and recursive encoder. We precisely define active distances and their distance spectrum for the code. Unique distance properties allow us to construct estimates for error bursts probabilities and for the probability of erroneous decoding of the convolutional code. We derive upper and lower estimates for error burst probabilities. Based on these expressions we suggest upper and lower bounds for FER performance.

B01-09

### Generator Polynomial Matrices of Reversed and Reversible Quasi-Cyclic Codes

*Ramy Taki ElDin, Hajime Matsui*

Quasi-cyclic (QC) codes over the finite field $\mathbb{F}_q$ correspond to certain $\mathbb{F}_q[x]$-modules. We describe a QC code $\mathcal{C}$ by a generator polynomial matrix. The code obtained by reversing the codewords of $\mathcal{C}$ is called the reversed code of $\mathcal{C}$ and denoted by $\mathcal{R}$. If $\mathcal{R} = \mathcal{C}$, then $\mathcal{C}$ is a reversible code. In this work, we prove a formula for a generator polynomial matrix of the reversed code $\mathcal{R}$ of a prescribed QC code $\mathcal{C}$. Then, we present a necessary and sufficient condition in terms of the proven formula to ensure the reversibility of any QC code. Moreover, we characterize the reduced generator polynomial matrices of reversible QC codes. As an application, we apply our theoretical results to QC codes with the best known parameters. Computer search is used to show the existence of reversible QC codes that achieve the upper bounds on the minimum distance of linear codes. Several binary reversible QC codes with the best known parameters are provided.

B01-10

### A Construction of Binary Punctured Linear Codes and A Supporting Method for Best Code Search

*Takuya Ohara, Makoto Takita, Masakatu Morii*

Reduction of redundancy and improvement of error-correcting capability are essential research themes in the coding theory. The best codes constructed in various ways are recorded in a database maintained by Markus Grassl. In this paper, we propose an algorithm to construct the best code using punctured codes and a supporting method for constructing the best codes. First, we define a new evaluation function to determine deletion bits and propose an algorithm for constructing punctured linear codes. 36 best codes were constructed in the proposed algorithm, and 131 best codes were constructed by further modifying those best codes. Secondly, we evaluate the possibility of increasing the minimum distance based on the relationship between code length, information length, and minimum distance. We narrowed down the target (n, k) code to try the best code search based on the evaluation and found 30 other best codes.

B01-11

### Decoder Error Propagation Mitigation for Spatially Coupled LDPC Codes

*Min Zhu, David G. M. Mitchell, Michael Lentmaier, Daniel J. Costello, Jr.*

In this paper, we introduce two new methods of mitigating decoder error propagation for low-latency sliding window decoding (SWD) of spatially coupled low-density parity-check (SC-LDPC) codes. Building on the recently introduced idea of check node (CN) doping of regular SC-LDPC codes, here we employ variable node (VN) doping to fix (set to a known value) a subset of variable nodes in the coupling chain. Both of these doping methods have the effect of allowing SWD to recover from error propagation, at a cost of a slight rate loss. Experimental results show that, similar to CN doping, VN doping improves performance by up to two orders of magnitude compared to un-doped SC-LDPC codes in the typical signal-to-noise ratio operating range. Further, compared to CN doping, VN doping has the advantage of not requiring any changes to the decoding process. In addition, a log-likelihood-ratio based window extension algorithm is proposed to reduce the effect of error propagation. Using this approach, we show that decoding latency can be reduced by up to a significant fraction without suffering any loss in performance.

## Algebraic Codes

B02-01

### Finding Self-Dual Quasi-Cyclic Codes with Large Minimum Weight via Polynomial Matrices

*Masaki Kawaguchi, Hajime Matsui*

In this paper, we search for a class of self-dual quasi-cyclic (QC) codes over binary field with large minimum weight. We employ generator polynomial matrices to specify a QC code because there is a condition for them to be a self-dual code. By combining factorization and Chinese remainder theorem, we efficiently search for these codes. Moreover, under certain conditions, we use a method of reciprocal polynomials to make them more efficient. We construct self-dual QC codes whose cycle length is 5, 7 and 9, and find them with the best minimum weight in each condition.

B02-02

### Algebraic List Decoding of Elliptic Codes Through Module Basis Reduction

*Yunqi Wan, Li Chen, Fangguo Zhang*

Elliptic codes is an important class of algebraic-geometric (AG) codes due to their least genus penalty. Their codeword length can exceed that of Reed-Solomon (RS) codes defined over the same finite field, resulting in a greater error-correction capability. This paper proposes the module basis reduction (BR) technique for solving the interpolation problem in algebraic list decoding (ALD) of one-point elliptic codes. A basis of the module that satisfies all interpolation constrains can be constructed by defining the explicit Lagrange interpolation function over the elliptic function field. They lead to the generators for the module basis. The basis can be further reduced to the desired Gröbner basis which contains the minimum interpolation polynomial Q(x, y, z). Compared with Koetter's interpolation, the BR interpolation technique significantly reduces the complexity in finding Q(x, y, z). Our analysis shows the BR interpolation complexity will reduce as the code rate increases.

B02-03

### An Iterative Bit-Flipping Decoding Algorithm For Binary Reed-Muller Codes

*Yong-Ting Ni, Cheng-Yu Pai, Chao-Yu Chen*

This paper presents an iterative bit-flipping (BF) decoding algorithm for binary Reed-Muller (RM) codes. The BF decoding algorithm is a hard-decision decoding algorithm. According to the updated hard reliability measures, one bit of the received hard-decision sequence is flipped at a time in each iteration. The simulation results show that the proposed BF decoding algorithm outperforms the conventional hard-decision majority decoding.

## Polar Codes

B03-01

### On the dependency between the code symmetries and the decoding efficiency

*Kirill Ivanov, Ruediger L Urbanke*

A framework of monomial codes is considered, which includes linear codes generated by the evaluation of certain monomials. Polar and Reed-Muller codes are the two best-known representatives of such codes and can be considered as two extreme cases. Reed-Muller codes have a large automorphism group but their low-complexity maximum likelihood decoding still remains an open problem. On the other hand, polar codes have much less symmetries but admit the efficient near-ML decoding.

We study the dependency between the code symmetries and the decoding efficiency. We introduce a new family of codes, partially symmetric monomial codes. These codes have a smaller group of symmetries than the Reed-Muller codes and are in this sense ”between” RM and polar codes. A lower bound on their parameters is introduced along with the explicit construction which achieves it. Structural properties of these codes are demonstrated and it is shown that they often have a recursive structure.

B03-02

### Complexity-efficient Fano Decoding of Polarization-adjusted Convolutional (PAC) Codes

*Mohammad Rowshan, Andreas Burg, Emanuele Viterbo*

Polarization-adjusted convolutional (PAC) codes are modified polar codes in which a one-to-one convolutional transformation is employed before the classical polar transform. Fano decoding of PAC codes in the Shannon lecture at ISIT2019 showed an outstanding performance at the cost of a high time-complexity, particularly at low SNR regimes. In order to reduce this complexity, an adaptive heuristic metric is proposed that improves the comparability of the variable-length paths and adjusts itself in response to the channel noise level. This metric can significantly reduce the number of nodes visited on average in tree-traversal. Additionally, a partial rewinding of the successive cancellation process is proposed to efficiently compute the intermediate LLRs and partial sums when backtracking occurs in the Fano algorithm. This method avoids storing the intermediate results of the decoding process or restarting (full rewinding) the decoding process.

## LDPC Codes

B04-01

### Decoding LDPC Codes with Probabilistic Local Maximum Likelihood Bit Flipping

*Rejoy Roy Mathews, Chris Winstead*

Low-density parity-check (LDPC) codes are high-performance linear error correcting codes with application to communication channels and digital storage media. LDPC codes are decoded using graph algorithms wherein a channel message sample is decoded with the aid of information from its adjacent graph neighborhood, called the syndrome. This work studies the conditional probability of a channel error given syndrome information at a particular decoding iteration to formulate a new algorithm called Probabilistic Local Maximum Likelihood Bit Flipping (PLMLBF). The PLMLBF algorithm uses a three dimensional Multi-iteration Probability Flip Matrix (MIPFM) to quantify the frequency of errors in a noise corrupted message frame being decoded using a specific LDPC code. The matrix is used to probabilistically decode noise corrupted message frames. The motivation for this work is to provide a theoretical framework for constructing probabilistic and noisy bit-flipping algorithms, such as the Noisy Gradient Descent Bit Flipping (NGDBF) algorithm, which up to now have been mainly heuristic in nature.

B04-02

### A Design of Differentially Encoded LDPC Coding Based on Multi-Edge Framework

*Yung-Tsao Hsu, Mao-Chao Lin*

We propose to optimize the design of a system of which the transmitter is composed of a low-density parity-check (LDPC) code followed by differential encoding (DE). The DE is included to remove the phase ambiguity in channel estimates. To achieve low complexity and/or high efficiency in channel estimation and also an acceptable performance in transmission, we optimize the outer LDPC code by considering the DE-LDPC code as a multi-edge type LDPC (MET-LDPC) code. The advantage of the proposed approach is verified by both the asymptotic behaviour and the finite-length simulation.

B04-03

### The 5G New Radio Code: Elementary Absorbing Sets and Error Floor Performance

*Masoome Otarinia, Thomas E Fuja*

The data channels in the 5G New Radio use quasi-cyclic low-density parity check (LDPC) codes for error control. Such codes, when used with a practical quantizer and an iterative decoder, typically have an error floor that is strongly impacted by absorbing sets present in the code's structure. This paper leverages the particular structure found in the 5G code to describe a simple means of identifying its (elementary) absorbing sets and describes an algorithm for finding them. It then uses simulation results to show which of the absorbing sets are responsible for the error floor performance for a particular choice of code and quantizer parameters.

B04-04

### Performance of Non-Binary LDPC Codes on Two-Dimensional Array Erasure Models

*Gou Hosoya, Toshihiro Niinomi*

In this study, we evaluate the performance of non-binary low-density parity-check (NB-LDPC) codes on two-dimensional array erasure models. For this channel model, two configurations of the codes on an array of storage devices are considered. We also present the density evolution of the proposed NB-LDPC code ensembles based on the above two configurations. The numerical and simulation results show that the proposed NB-LDPC codes outperform the conventional NB-LDPC codes.

B04-05

### Encoding Algorithm of Binary and Non-binary Irregular LDPC Codes via Block Triangular Matrices with Low Weight Diagonal Submatrices

*Yuta Iketo, Takayuki Nozaki*

In this paper, we propose a low complexity encoding algorithm for the binary and non-binary irregular LDPC codes. This algorithm transforms the parity part of the parity-check matrix into a block triangular matrix by row and column permutations. By lowering the weight of diagonal submatrices, we reduce the encoding complexity.

B04-06

### Analysis of UEP QC-LDPC Codes Using Density Evolution

*Yi-Hsuan Chen, Yu-Ting Liu, Chung-Hsuan Wang, Chi-chao Chao*

We develop asymptotic analysis of recently constructed unequal error protection (UEP) quasi-cyclic (QC) low-density parity-check (LDPC) codes by using density evolution and its Gaussian approximation in this paper. The proposed analysis can indeed yield different decoding thresholds for different protection levels. As verified by computer simulation, the coding gain differences between protection levels can also be well predicted.

B04-07

### NB-LDPC Codes with High Rates Achieving Low BER over the AWGN Channel with QAM Signaling

*Gada Rezgui, Asma Maaloui, Iryna Andriyanova, Charly Poulliat, Cyril Measson*

The paper investigates high-rate Low-Density-Parity-Check (LDPC) codes, able to achieve a low bit error rate (BER). Such an operational regime of LDPC codes finds its application in optical transmissions. For this reason the considered transmission model is the one close to optical communications: it is a M-ary Quadrature-Amplitude Modulation (QAM) signaling over the M-ary input additive Gaussian channel. We study three main points: a) which LDPC codes of fixed codelength can achieve low BER for a code rate R¿0.8; b) whether non-binary LDPC (NB-LDPC) codes, defined over GF(Q), are efficient in this setting; c) how to keep a reasonable decoding complexity for a given modulation order. Our performance analysis is complete and it is based on the calculation of the average bit error rate of a given ensemble, by using both asymptotic and finite-length tools of sparse-graph codes. Our results show that NB-LDPC codes with moderate values of Q, together with a Symbol Interleaved Coded Modulation (SICM) approach, offer the best performance at low BER.

## Coding for Storage

B05-01

### Bonds of Constrained Systems and Their Characteristics

*Akiko Manada, Takahiro Ota, Hiroyoshi Morita*

A constrained system is a set of words satisfying some constraints on the appearance of subwords, and the study on constrained systems is the core of the study on constrained coding. The notion of constrained coding has been often applied in data storage media to reduce the likelihood of errors.

Given data sequences satisfying some constraints, it is not always possible to directly concatenate the data sequences so that the resulting sequence also satisfies the constraints. In this paper, we define a bond to be a sequence that can concatenate any allowed data sequences without violating the constraints, and present a necessary and sufficient condition on the existence of a bond. We also discuss on the length of a bond and the complexity of finding a bond, together with some examples of bonds.

B05-02

### Repair of Multiple Descriptions on Distributed Storage

*Anders Høst-Madsen, Heecheol Yang, Minchul Kim, Jungwoo Lee*

In multiple descriptions on distributed storage, a source is stored in a shared fashion on multiple servers. When a subset of servers are contacted, the source should be estimated with a certain maximum distortion depending on the number of servers. The problem considered in this paper is how to restore the system operation when one of the servers fail and a new server replaces it, that is, repair. The requirement is that the distortions in the restored system should be no more than in the original system. The question is how many extra bits are needed for repair. We find the optimum solution for a two server problem in the Gaussian case, and an achievable rate for general n nodes. One conclusion is that it is necessary to design the multiple description codes with repair in mind.

B05-03

### Cooperative Locality and Availability of the MacDonald Codes for Multiple Symbol Erasures

*Zhi Jing, Hong-Yeop Song*

We calculate the cooperative locality $r_2$ for 2-symbol repair and all-symbol availability $t$ for single symbol repair of some MacDonald codes. We also show that the MacDonald codes are optimal only when $k = 3$ and 4 with respect to the bounds of availability by Tamo-Barg and Wang-Zhang.

B05-04

### Segmented Reverse Concatenation: A New Approach to Constrained ECC

*Ryan Gabrys, Paul H. Siegel, Eitan Yaakobi*

In this work, a new coding scheme called segmented reverse concatenation is described, which generates constrained codes that can also correct a prescribed number of errors. Our codes are based upon the generalized reverse concatenation method; however, the key difference between our scheme and prior art is that in our scheme the redundancy symbols of the code are able to be partitioned into disjoint segments, each of which requires only a single parity bit to maintain the minimum distance of the code. We consider three potential applications of the new technique, and it is shown that in all three cases our approach improves upon prior art. Our scheme can be applied to many setups, although it is particularly well-suited for scenarios where the constrained encoder has a high information rate.

B05-05

### A Note on a Relationship between Smooth Locally Decodable Codes and Private Information Retrieval

*Koki Kazama, Akira Kamatsuka, Takahiro Yoshida, Toshiyasu Matsushima*

We focus on smooth locally decodable codes (SLDC) and Private Information Retrieval (PIR). Recently, a relationship between SLDC and PIR are studied using information theoretical notations. In this paper, we clarify a relationship between SLDCs and PIR using set theoretical notations mainly.

B05-06

### Rack-Aware Cooperative Regenerating Codes

*Shreya Gupta, V. Lalitha*

In distributed storage systems, cooperative regenerating codes tradeoff storage for repair bandwidth in the case of multiple node failures. In rack-aware distributed storage systems, there is no cost associated with transferring symbols within a rack. Hence, the repair bandwidth will only take into account cross-rack transfer. Rack-aware regenerating codes for the case of single node failures have been studied and their repair bandwidth tradeoff characterized. In this paper, we consider the framework of rack-aware cooperative regenerating codes for the case of multiple node failures where the node failures are uniformly distributed among a certain number of racks. We characterize the storage repair-bandwidth tradeoff as well as derive the minimum storage and minimum repair bandwidth points of the tradeoff. We also provide constructions of minimum bandwidth rack-aware cooperative regenerating codes for all parameters.

B05-07

### Achievable Rates of Concatenated Codes in DNA Storage under Substitution Errors

*Andreas Lenz, Lorenz Welter, Sven Puchinger*

In this paper, we study achievable rates of concatenated coding schemes over a deoxyribonucleic acid (DNA) storage channel. Our channel model incorporates the main features of DNA-based data storage. First, information is stored on many, short DNA strands. Second, the strands are stored in an unordered fashion inside the storage medium and each strand is replicated many times. Third, the data is accessed in an uncontrollable manner, i.e., random strands are drawn from the medium and received, possibly with errors. As one of our results, we show that there is a significant gap between the channel capacity and the achievable rate of a standard concatenated code in which one strand corresponds to an inner block. This is in fact surprising as for other channels, such as q-ary symmetric channels, concatenated codes are known to achieve the capacity. We further propose a modified concatenated coding scheme by combining several strands into one inner block, which allows to narrow the gap and achieve rates that are close to the capacity.

## Insertions/Deletions Correcting Codes

B06-01

### Conversion Method from Erasure Codes to Multi-Deletion Error-Correcting Codes for Information in Array Design

*Manabu Hagiwara*

This paper considers error-correction for information in array design, i.e., two-dimensional design such as is used in QR-codes. The error model is multi-deletion errors. In particular, row-deletions and column-deletions are considered. The main result is to provide a conversion method that converts two erasure codes to a multi-deletion error-correcting code.

B06-02

### Optimal Reconstruction Codes for Deletion Channels

*Johan Chrisnata, Han Mao Kiah, Eitan Yaakobi*

The sequence reconstruction problem, introduced by Levenshtein in 2001, considers a communication scenario where the sender transmits a codeword from some codebook and the receiver obtains multiple noisy reads of the codeword. Motivated by modern storage devices, we introduced a variant of the problem where the number of noisy reads $N$ is fixed (Kiah et al. 2020). Of significance, for the single-deletion channel, using $\log_2 \log_2 n + O(1)$ redundant bits, we designed a codebook of length $n$ that reconstructs codewords from two distinct noisy reads.

In this work, we show that $\log_2 \log_2 n - O(1)$ redundant bits are necessary for such reconstruction codes, thereby, demonstrating the optimality of our previous construction. Furthermore, we show that these reconstruction codes can be used in $t$-deletion channels (with $t \geq 2$) to uniquely reconstruct codewords from $n^{t-1} + O\left(n^{t-2}\right)$ distinct noisy reads.

B06-03

### Decoding Algorithms of Monotone Codes and Azinv Codes and Their Unified View

*Hokuto Takahashi, Manabu Hagiwara*

This paper investigates linear-time decoding algorithms for two classes of error-correcting codes. One of the classes is monotone codes which are known as single deletion codes. The other is azinv codes which are known as single balanced adjacent deletion codes. As results, this paper proposes generalizations of Levenshtein's decoding algorithm for Levenshtein's single deletion codes. This paper points out that it is possible to unify our new two decoding algorithms.

B06-04

### Polar Coding for Oversampling Drift Channel

*Leo Otani, Haruhiko Kaneko*

Oversampling could be effective technique to reduce error probability in timing-drift channel, wherein synchronization errors occur at a granularity finer than one bit. Also the oversampling will be feasible in some new storage devices with relatively slow media speed, such as DNA storage with nanopore sequencing. This paper defines timing-drift channel with oversampling, namely oversampling drift channel (OsDC), and presents error correction by polar code with a successive cancellation decoding adapted to the OsDC. Computer simulation shows estimation of symmetric capacity of polar bit channel, and also shows that the code rate can be improved by increasing the oversampling factor.

B06-05

### Encoding Algorithm for Run-Length Limited Single Insertion/Deletion Correcting Code

*Reona Takemoto, Takayuki Nozaki*

Synchronization errors cause insertion and deletion errors in transmitted sequences. Schoeny et al. constructed codes correcting a burst of insertion or deletion error by employing a run-length limited single insertion/deletion correcting (RLL-SIDC) code and a bounded single insertion/deletion correcting code. To present an efficient encoding algorithm for the burst insertion/deletion correcting code, we need to provide one for an RLL-SIDC code. The purpose of this research is to provide an efficient encodable RLL-SIDC code and its encoding algorithm. In this paper, we construct a SIDC code which has a mechanism to limit the maximum run-length of the codeword. Moreover, we present its encoding algorithm.

B06-06

### Codes Correcting Bounded Length Tandem Duplication

*Kamilla Nazirkhanova, Luiza Medova, Stanislav Kruglik, Alexey A. Frolov*

In this paper we extend the problem of correcting a tandem duplication of a fixed number of symbols to the problem of correcting a tandem duplication of a bounded length. This type of error can be represented as a repetition of a symbols block. We propose the upper and the lower bounds on the cardinality based on the sphere-packing bound and constructions of codes correcting one tandem duplication of a bounded length based on Varshamov-Tenengolts code.

B06-07

### Criss-Cross Deletion Correcting Codes

*Rawad Bitar, Ilia Smagloy, Lorenz Welter, Antonia Wachter-Zeh, Eitan Yaakobi*

This paper studies the problem of constructing codes correcting deletions in arrays. Under this model, it is assumed that an $n \times n$ array can experience deletions of rows and columns. These deletion errors are referred to as $(t_r, t_c)$-criss-cross deletions if $t_r$ rows and $t_c$ columns are deleted, while a code correcting these deletion patterns is called a $(t_r, t_c)$-criss-cross deletion correcting code. The definitions for criss-cross insertions are similar.

Similar to the one-dimensional case, it is first shown that the problems of correcting criss-cross deletions and criss-cross insertions are equivalent. Then, we mostly investigate the case of $(1, 1)$-criss-cross deletions. An asymptotic upper bound on the cardinality of $(1, 1)$-criss-cross deletion correcting codes is shown which assures that the asymptotic redundancy is at least $2n - 2 + 2\log n$ bits. Finally, a code construction with an explicit decoding algorithm is presented. The redundancy of the construction is away from the lower bound by at most $2\log n + 9 + 2\log e$ bits.

## Information Theory and Biology

B07-01

### A Coding Theory Perspective on Multiplexed Molecular Profiling of Biological Tissues

*Luca DAlessio, Litian Liu, Ken R. Duffy, Yonina C. Eldar, Muriel Médard, Mehrtash Babadi*

High-throughput and quantitative experimental technologies are experiencing rapid advances in the biological sciences. One important recent technique is multiplexed fluorescence in situ hybridization (mFISH), which enables the identification and localization of large numbers of individual strands of RNA within single cells. Core to that technology is a coding problem: with each RNA sequence of interest being a codeword, how to design a codebook of probes, and how to decode the resulting noisy measurements? Published work has relied on assumptions of uniformly distributed codewords and binary symmetric channels for decoding, and to a lesser degree for code construction. Here we establish that both of these assumptions are inappropriate in the context of mFISH experiments and substantial decoding performance gains can be obtained by using more appropriate, less classical, assumptions. We propose a more appropriate asymmetric channel model that can be readily parameterized from data and use it to develop a maximum a posteriori (MAP) decoders. We show that false discovery rate for rare RNAs, which is the key experimental metric, is vastly improved with MAP decoders even when employed with the existing suboptimal codebook. Using an evolutionary optimization methodology, we further show that by permuting the codebook to better align with the prior, which is an experimentally straightforward procedure, significant further improvements are possible.

## Index Coding

B08-01

### Independent User Partition Multicast Scheme for the Groupcast Index Coding Problem

*Arman Sharififar, Neda Aboutorab, Yucheng Liu, Parastoo Sadeghi*

The groupcast index coding (GIC) problem is a generalization of the index coding problem, where one packet can be demanded by multiple users. In this paper, we propose a new coding scheme called independent user partition multicast (IUPM) for the GIC problem. The novelty of this scheme compared to the user partition multicast (UPM) (Shanmugam et al., 2015) is in removing redundancies in the UPM solution by eliminating the linearly dependent coded packets. We also prove that the UPM scheme subsumes the packet partition multicast (PPM) scheme (Tehrani et al., 2012). Hence, the IUPM scheme is a generalization of both PPM and UPM schemes. Furthermore, inspired by jointly considering users and packets, we modify the coded approximation partition multicast (CAPM) scheme (Unal and Wagner, 2016) to achieve a new polynomial-time algorithm for solving the general GIC problem. We characterize a class of GIC problems with $frack(k-1)2$ packets, for any integer $k \geq 2$, for which the IUPM scheme is optimal. We also prove that for this class, the broadcast rate of the proposed new heuristic algorithm is $k$, while the broadcast rate of the CAPM scheme is $\mathcal{O}(k^2)$.

B08-02

### Secure Index Coding with Security Constraints on Receivers

*Yucheng Liu, Parastoo Sadeghi, Neda Aboutorab, Arman Sharififar*

Index coding is concerned with efficient broadcast of a set of messages to receivers in the presence of receiver side information. In this paper, we study the secure index coding problem with security constraints on the receivers themselves. That is, for each receiver there is a single legitimate message it needs to decode and a prohibited message list, none of which should be decoded by that receiver. To this end, our contributions are threefold. We first introduce a secure linear coding scheme, which is an extended version of the fractional local partial clique covering scheme that was originally devised for non-secure index coding. We then develop two information-theoretic bounds on the performance of any valid secure index code, namely secure polymatroidal outer bound (on the capacity region) and secure maximum acyclic induced subgraph lower bound (on the broadcast rate). The structure of these bounds leads us to further develop two necessary conditions for a given index coding problem to be securely feasible (i.e., to have nonzero rates).

## Network Coding and Information Theory

B09-01

### A Simple Capacity Outer Bound for Two-Way Channels and Capacity Approximation Results

*Jian-Jia Weng, Fady Alajaji, Tamas Linder*

Channel symmetry properties that imply the tightness of Shannon's random coding inner bound have recently been used to determine the capacity region of discrete-memoryless two-way channels (DM-TWCs). For channels without such symmetry properties, outer bounds are often needed to estimate the capacity region. However, validating symmetry conditions and/or evaluating non-trivial outer bounds are computationally demanding, especially for channels with large input and output alphabets. In this paper, three easy-to-check conditions that identify DM-TWCs with no such symmetry properties as well as an easy-to-compute outer bound are derived. The bound is obtained from Shannon's inner bound computation but is non-trivial. Using this outer bound, approximate capacity results can be established for certain DM-TWCs. The results are illustrated by two examples.

## Quantum Error Correction

B10-01

### Single Quantum Deletion Error-Correcting Codes

*Ayumu Nakayama, Manabu Hagiwara*

In this paper, we discuss a construction method of quantum deletion error-correcting codes. First of all, we define deletion errors for quantum states, an encoder, a decoder, and three conditions that are expressed by only the combinatorial language. Then, we prove that quantum deletion error-correcting codes can be constructed by two sets that satisfy the conditions. In other words, problems that correct the deletion errors for quantum states are reduced to problems that find the sets satisfying the condition by this paper. Also, we experimented with the codes over IBM Quantum Experience.

B10-02

### New Instances of Quantum Error-Correcting Codes for Single Deletion Errors

*Taro Shibayama*

This paper provides new instances of quantum error-correcting codes. According to recent results by Nakayama and Hagiwara, by using two sets of binary sequences that satisfy three conditions, we can construct quantum error-correcting codes for single deletion errors. However, only two instances of two sets that satisfy the three conditions have been found to date. The present study constructs two infinite series of sets that satisfy the three conditions. In other words, this paper constructs new infinite series of quantum error-correcting codes for single deletion errors.

## Cryptography

C01-01

### Structurally aggregate message authentication codes

*Yuta Ishii, Mitsuru Tada*

In an aggregate MAC scheme, plural (single) tags can be put together so that we can decrease the tag size and thereby the communication cost. The aggregation ways are classified roughly into two types, parallel-type aggregations and serial-type ones. In the former-type ones, a valid aggregate tag does not refer to, so far, the order for generating the single tags to make the aggregate tag, whereas in the latter-type ones, a valid aggregate tag can assure the generating order. Then we can see the former-type ones in [4], [6] and the latter-type ones in [3], [5]. In this paper, we extend those schemes, and present an aggregate MAC scheme in which a valid aggregate tag can assure the structural generating orders which can be represented by a series-parallel graph, and show the security for the proposed scheme.

C01-02

### The time-adaptive statistical testing for random number generators

*Boris Ryabko, Viacheslav Zhuravlev*

The problem of constructing effective statistical tests for random number generators (RNG) is considered. Currently, there are hundreds of RNG statistical tests that are often combined into so-called batteries, each containing from a dozen to more than one hundred tests. When a battery test is used, it is applied to a sequence generated by the RNG, and the calculation time is determined by the length of the sequence and the number of tests. Generally speaking, the longer the sequence, the smaller deviations from randomness can be found by a specific test. So, when a battery is applied, on the one hand, the "better" tests are in the battery, the more chances to reject a "bad" RNG. On the other hand, the larger the battery, the less time can be spent on each test and, therefore, the shorter the test sequence. In turn, this reduces the ability to find small deviations from randomness. To reduce this trade-off, we propose an adaptive way to use batteries (and other sets) of tests that can be used in such a way as to increase the testing power.

C01-03

### On the Power of Interaction in Signcryption

*Junichi Ida, Junji Shikata, Yohei Watanabe*

Signcryption (SC) achieves the goal with lower computational costs than simply combining public-key encryption (PKE) and digital signatures (DS). Meanwhile, at SCN 2014, Dodis and Fiore formalized interactive PKE and DS. In particular, in the interactive setting, they showed a CCA-secure PKE scheme can be constructed assuming only CPA-secure PKE schemes in a black-box manner.

In this paper, we focus on SC schemes in the interactive setting (ISC for short). Specifically, we newly define a model and security notions for ISC schemes. We then propose generic constructions of ISC schemes by using CPA-secure PKE schemes rather than CCA-secure ones, whereas such a realization is unknown in the context of non-interactive SC schemes. We show that two rounds are sufficient to construct an ISC scheme from only CPA-secure PKE schemes. Furthermore, we also show the first SC scheme that can be efficiently instantiated from simple assumptions in the standard model without pairings or lattices by allowing interaction.

C01-04

### A Construction of Robustly Reusable Fuzzy Extractors over Blockchains

*Kodai Sato, Kenji Yasunaga, Toru Fujiwara*

Fuzzy extractors (FEs) turn a noisy source of high entropy, such as biometric information, into a uniformly distributed key. FEs can extract cryptographically desirable keys without storing the keys. FE was first proposed by Dodis et al., and it has been studied actively since. Moreover, a robust FE to achieve higher security and a reusable FE to achieve more functionality were proposed. Wen et al. constructed a robustly reusable FE (rrFE) that satisfies robustness and reusability simultaneously. However, only few rrFEs have been proposed and all are based on the Common Reference String (CRS) model. Recently, Goyal and Goyal defined blockchain formally as a model for use as components of cryptographic protocols. In this paper, we introduce an rrFE based on the blockchain proposed by Goyal et al. instead of the CRS model. In contrast to the CRS model, a blockchain trusts not a specific third party but a distributed system. Therefore, a protocol based on CRS may lose security by a betrayal of TTP. Meanwhile, our protocol tolerates malicious acts of parties as long as the majority are honest.

C01-05

### The Existence of Cycles in the Supersingular Isogeny Graphs Used in SIKE

*Hiroshi Onuki, Yusuke Aikawa, Tsuyoshi Takagi*

In this paper, we consider the structure of isogeny graphs in SIDH, that is an isogeny-based key-exchange protocol. SIDH is the underlying protocol SIKE, which is one of the candidates for NIST post quantum cryptography standardization, SIKE. Since the security of SIDH is based on the hardness of the path-finding problem in isogeny graphs, it is important to study those structure. The existence of cycles in isogeny graph is related to the path-finding problem, so we investigate cycles in the graphs used in SIKE. In particular, we focus on SIKEp434 and SIKEp503, which are the parameter sets of SIKE claimed to satisfy the NIST security level 1 and 2, respectively. We show that there are two cycles in the 3-isogeny graph in SIKEp434, and there is no cycles in the other graphs in SIKEp434 and SIKEp503.

C01-06

### Delegatable proof of knowledge systems

*Naoya Shiratori, Mitsuru Tada*

In this paper, we propose the concept of delegatable proofs of knowledge (DPoK). A delegatable proof of knowledge enables a prover to delegate its proving work to another party instead of doing that itself. If the prover delegates the work to any party, the delegated party can prove the prover's statement to the verifier, however, it cannot compute the prover's secret. We present the concrete example of DPoK proven secure in the standard model.

C01-07

### Hamming Weight of Product of Random Sparse Polynomials

*Akinori Kawachi*

Consider two random $n$-bit vectors $x$,$y$ of which each coordinate is 1 with small probability $e$ independently from the others. It is easy to see that the Hamming weight of their sum $x + y$ is strongly concentrated around the expectation by the standard probability analysis for independent random variables such as the Chernoff bounds, that is, $wt(x + y)$ is between $1.1E[wt(x + y)]$ and $0.9E[wt(x + y)]$ with probability $1 - exp(-\Omega(en))$, where $E[wt(x + y)] = 2e(1 - e)$. In this paper, we focus on the Hamming weight of their "product" $x * y$ defined as a product of polynomials over the ring $F_2[t]/(t^n - 1)$, which is utilized for construction of the post-quantum public-key encryption scheme HQC [Aguilar Melchor, et al. IEEE Trans. (2018)]. In the case of the product, the standard analysis does not work because of correlations among the coordinates of $x * y$. We prove weak concentration bounds for the Hamming weight of $x * y$ from Chebyshev's inequality by analyzing the correlations. For example, we can show that $x * y$ is between $1.1E[wt(x * y)]$ with probability $1 - O(e^3 n)$ for $e = \Omega(n^{-1/2})$ from the bounds, where $E[wt(x * y)] = (1 - (1 - 2e^2)^n)n/2$.

C01-08

### The relation between Proportion test and Uniformity test in NIST SP800-22

*Atsushi Iwasaki*

NIST SP800-22 statistical test tool is one of the randomness test suites. It consists of 15 kinds of tests, and each test outputs the p-value for a sequence. Each test outputs multiple p-values when we test plural sequences. SP800-22 suggests to perform additional hypothesis tests for the multiple p-values, called the proportion test and the uniformity test, and judge the randomness of the tested sequences. To make a rational criterion for the two tests, the relation between the proportion test and the uniformity test is essential. In this paper, we derive the probability that both the proportion and uniformity tests simultaneously reject the null hypothesis. In the derivation process, we use a numerical method, but it is not a stochastic algorithm. Thus, we can ensure the properness of the derived value of the probability.

C01-09

### How to Detect Malicious Behaviors in a Card-Based Majority Voting Protocol with Three Inputs

*Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta*

Card-based protocol is a multi-party computation using cards. The card-based protocol using operations called private operation has an advantage that the number of cards and the number of times of communication are smaller than the card-based protocol using operations called shuffle. However, there is a disadvantage that private operation allows dishonest players to perform malicious behaviors. Although the method to detect malicious behaviors in private operations was proposed, the method was available only in committed-format protocols, where inputs and outputs are represented by a pair of cards called commitment. In this paper, we show how to detect malicious behaviors in non-committed-format protocol with an example of a three-input majority voting protocol using private operations. Our majority voting protocol requires a smaller number of cards than the minimum number of cards required for committed-format protocols.

C01-10

### A Key Recovery Algorithm Using Random Key Leakage from AES Key Schedule

*Tomoki Uemura, Yohei Watanabe, Yang Li, Noriyuki Miura, Mitsugu Iwamoto, Kazuo Sakiyama, Kazuo Ohta*

A key recovery algorithm using parts of the key schedules is proposed for evaluating the threat of probing attack. Suppose that we have an information leakage sensor, and we can detect a leak (attacked) point where an attacker makes electrical/physical contact with a laser, a probe, etc. We assume that the attacked bits (leaked bits) are completely known to the attacker, whereas the other non-attacked bits are not leaked at all. We also assume that each bit leaks with a constant probability. Our key recovery algorithm is constructed by modifying the pruning phase that for cold boot attacks proposed by Tsow. Experimental result shows that, using our algorithm, more than 15% leakage recovers the key with almost probability 1, whereas less than 10% is recovered with small probability close to 0.

C01-11

### Client-Aided Bit-Composition Protocol with Guaranteed Output Delivery

*Hikaru Tsuchida, Takashi Nishide*

Secure multiparty computation (MPC) enables parties to compute an arbitrary function without revealing each party's inputs. A typical MPC is the secret sharing based MPC (SS-MPC). In the SS-MPC, each party distributes its inputs, and the computation proceeds with secret shares that just look like random numbers distributed among the parties. In the SS-MPC protocol, the parties can compute any function represented as a circuit by using shares locally and communicating among the parties. In particular, when the parties compute a complex function composed of binary and arithmetic circuits, an efficient share conversion protocol facilitates the computation of it. An important conversion protocol is the bit-composition protocol that converts a $k$-dimensional vector with the shares on $\mathbb{Z}_2$ (i.e., shares of binary sequence) to the shares on $\mathbb{Z}_{2^k}$ (i.e., shares of decimal value). The previous work proposed a maliciously secure bit-composition protocol with guaranteed output delivery (GOD), which is the security notion that all the parties learn the correct output regardless of the attacker's behaviour. However, its security is proved in the random oracle model.

In this paper, we propose a new bit-composition protocol with GOD by introducing additional clients just helping the parties during computation. Our protocol is based on a maliciously secure four-party protocol with one corruption using replicated secret sharing. The security of our protocol is proved in the standard model (which is weaker than the random oracle model). Our protocol achieves the efficiency and strongest security simultaneously. We also propose a protocol for the Hamming distance with GOD by modifying our bit-composition protocol. It achieves a secure iris recognition service via MPC with GOD.

## Information-Theoretic Security

C02-01

### Information leakage through passive timing attacks on RSA decryption system

*Tomonori Hirata, Yuichi Kaji*

The threat of timing attacks is especially serious when an attacker actively controls the input to a target program. Countermeasures are studied to deter such active attacks, but the attacker still has the chance to learn something about the concealed information by passively watching the running time of the target program. The risk of passive timing attacks can be measured by the mutual information between the concealed information and the running time. However, the computation of the mutual information is hardly possible except for toy examples. This study focuses on three algorithms for RSA decryption, derives formulas of the mutual information under several assumptions and approximations, and calculates the mutual information numerically for practical security parameters.

C02-02

### On the Capacity of Gaussian Multiple-Access Wiretap Channels with Feedback

*Bin Dai, Chong Li, Yingbin Liang, Zheng Ma, Shlomo (Shitz) Shamai*

Two-user Gaussian multiple-access wiretap channel models with feedback are investigated. First, we show that the secrecy capacity regions of both the Gaussian multiple-access wiretap channel (GMAC-WT) with feedback and the GMAC-WT with noncausal channel state information at the transmitters (GMAC-WT-NCSIT) and feedback equal the capacity region of the Gaussian multiple-access channel (GMAC) with feedback and without the secrecy constraint and the state corruption. Next, we derive inner and outer bounds on the secrecy capacity region of the GMAC-WT with degraded message set and feedback. Our numerical results show that the perfect secrecy of the private message can be achieved without loss of any reliable transmission rate.

C02-03

### Scalable Security in Interference Channels With Arbitrary Number of Users

*Parisa Babaheidarian, Somayeh Salimi, Panagiotis Papadimitratos*

In this paper, we present an achievable security scheme for an interference channel with arbitrary number of users. In this model, each receiver should be able to decode its intended message while it should remain ignorant regarding messages intended for other receivers. Our scheme relies on transmitters to collectively ensure the confidentiality of the transmitted messages using a cooperative jamming technique and lattice alignment. The Asymmetric compute-and-forward framework is used to perform the decoding operation. The proposed scheme is the first asymptotically optimal achievable scheme for this security scenario which scales to arbitrary number of users and works for any finite-valued SNR. Also, our scheme achieves the upper bound sum secure degrees of freedom of 1 without using external helpers and thus the achievable rates lie within constant gap from sum secure capacity.

C02-04

### A Capacity-achieving One-way Key Agreement with Improved Finite Blocklength Analysis

*Setareh Sharifian, Alireza Poostindouz, Reihaneh Safavi-Naini*

Information-theoretic secret key agreement (SKA) protocols are a fundamental cryptographic primitive that are used to establish a shared secret key between two or more parties. In a two-party SKA in source model, Alice and Bob have samples of two correlated variables that are partially leaked to Eve, and their goal is to establish a shared secret key by communicating over a reliable public channel. Eve must have no information about the established key. In this paper, we study the problem of one-way secret key agreement where the key is established by Alice sending a public message to Bob. We propose a one-way SKA (OW-SKA) protocol, prove that it achieves the one-way secret key capacity, and use it to derive a finite blocklength bound on the achievable secret key length. We compare our results with existing OW-SKAs and show the protocol achieves a longer key, and has a combination of desirable properties.

C02-05

### A Channel Model of Transceivers for Multiterminal Secret Key Agreement

*Alireza Poostindouz, Reihaneh Safavi-Naini*

Information theoretic secret key agreement is impossible without making initial assumptions. One type of initial assumption is correlated random variables that are generated by using a noisy channel that connects the terminals. Terminals use the correlated random variables and communication over a reliable public channel to arrive at a shared secret key. Previous channel models assume that each terminal either controls one input to the channel, or receives one output variable of the channel. In this paper, we propose a new channel model of transceivers where each terminal simultaneously controls an input variable and observes an output variable of the (noisy) channel. We give upper and lower bounds for the secret key capacity (i.e., highest achievable key rate) of this transceiver model, and prove the secret key capacity under the conditions that the public communication is noninteractive and input variables of the noisy channel are independent.

C02-06

### Biometric Identification Systems with Both Chosen and Generated Secrecy

*Vamoua Yachongka, Hideki Yagi*

We investigate the fundamental limits of a combined usage of chosen- and generated-secret keys for biometric identification systems with exponentially many users. The system consists of two phases: enrollment and identification phases. In the enrollment phase, for each user, the encoder generates a secret key and a helper data by using another secret key, chosen independently, and the bio-data sequence. In the identification phase, observing biometric data sequence, the decoder estimates index, chosen- and generated-secret keys of the identified user. In this study, the capacity region of identification, chosen- and generated-secrecy, template, and privacy-leakage rates of the system is characterized. The characterization shows that there is a trade-off among identification, chosen- and generated-secrecy rates, and greater values of identification and chosen-secrecy rates require larger storage space, but the generated-secrecy rate does not contribute to such increase. Also, this result includes various known results as special cases.

## Secret Sharing

C03-01

### Optimal Basis Matrices of a Visual Cryptography Scheme with Meaningful Shares and Analysis of Its Security

*Sekine Kyohei, Hiroki Koga*

The extended visual cryptography scheme (EVCS) proposed by Ateniese et al. is one variation of the visual cryptography scheme such that a secret image is recovered from certain qualified collections of meaningful shares that are distributed to respective participants. In this paper, we give a new definition of the EVCS for improving visibility of the recovered secret image as well as the shares. We construct optimal basis matrices with the minimum number of pixel expansion by solving a certain integer programming problem. We also analyze security of the EVCS meeting the new definition from information-theoretic viewpoint.

C03-02

### A Linear Algebraic Approach to Strongly Secure Ramp Secret Sharing for General Access Structures

*Reo Eriguchi, Noboru Kunihiro, Koji Nuida*

Secret sharing is a cryptographic technique to share a secret among participants in such a way that only authorized subsets are able to recover the secret. Ramp secret sharing schemes can achieve better information ratio than perfect schemes while some partial information on a secret which is composed of several sub-secrets leaks out. The notion of strong security has been introduced to control the amount of information on every subset of the sub-secrets unauthorized sets can obtain. In this paper, we reduce the construction of strongly secure ramp secret sharing for general access structures to a linear algebraic problem. As a result, we show that previous results on strongly secure network coding imply two constructions of a linear transformation which makes a given linear ramp scheme strongly secure. They are explicit or provide a deterministic algorithm while the previous method which works for any linear ramp scheme is probabilistic.

C03-03

### New Constructions of an Evolving 2-Threshold Scheme Based on Binary or D-ary Prefix Codes

*Ryo Okamura, Hiroki Koga*

Recently, Komargodski et al. proposed a nonconventional secret sharing scheme called an evolving $k$-threshold scheme. In the evolving k-threshold scheme, a dealer can generate infinitely many shares such that a secret is correctly decoded from arbitrary more than or equal to k shares while no information on the secret is revealed from any less than k shares. In this paper, we propose a new construction of an evolving 2-threshold scheme based on a binary prefix code for a secret with arbitrary length. In addition, we give a construction of an evolving 2-threshold scheme based on a $D$-ary prefix code, where $D \geq 3$ is an arbitrary integer. It is shown that the sizes of shares of this construction are more efficient than the binary case.

C03-04

### Compact Verifiably Multiplicative Secret Sharing

*Maki Yoshida, Satoshi Obana*

A $d$-multiplicative secret sharing ($d$-MSS) scheme over a finite field allows the players to multiply $d$ shared secrets without recovering the secrets by converting their shares *locally* into an *additive* sharing of the product [Journal of Cryptology, 2010]. A verifiably $d$-MSS ($d$-VMSS) further enables the players to locally generate an *additive* sharing of a *proof* that the output (rather than each share) is correct [IEEE Trans. on Information Theory, 2019]. In the most efficient construction known so far, while a share of the output is a single element of the finite field, a proof of correctness consists of two or more elements. In this paper, we study (in)feasibility of a single-element proof of correctness. First, we derive a sufficient condition on a proof-generation function, referred to as *multiplicative-only homomorphism (MoH).* Secondly, we show the concrete family of MoHs, meaning that the condition is satisfied. Then, we present a generic construction of $d$-VMSS from any $d$-MSS and any MoH. Finally, we show concrete instantiations of $d$-VMSS that realize a single-element proof of correctness.

C03-05

### Fourier-based Verifiable Function Secret Sharing

*Takeshi Koshiba*

Function secret sharing is a cryptographic protocol for secure distribution of a secret function. While the notion of function secret sharing is a conceptual extension of secret sharing schemes, it faces difficulties in its constructions. We demonstrate that if we consider function secret sharing schemes for Fourier basis functions then we can enjoy the linear properties of linear secret sharing schemes to construct function secret sharing schemes. In this paper, we construct a verifiable function secret sharing by using Fourier basis functions, where players can verify if the dealer is cheating.

## Sequences

C04-01

### A Parallel Blum-Micali Generator Based on the Gauss Periods

*Yuta Kodera, Tomoya Tatara, Takuya Kusaka, Yasuyuki Nogami, Satoshi Uehara*

In this paper, the authors propose an algorithm to generate a sequence of bits in parallel to enhance the generating performance of the Blum-Micali method which is for constructing a pseudorandom number generator. More precisely, since the classical definition needs to refer the previous state to generate the next bit, we modify the generation steps in an alternative way by introducing the feature of the Gauss periods. It gives us a unique representation of elements as if a primitive element generates those elements as the powers and this mechanism realizes the parallel algorithm. As a result, the generator achieves to mimic the main concept of the Blum-Micali method in parallel and it is thought to be secure if the discrete logarithm problem is hard to solve.

C04-02

### A Study on Randomness of Sequences Obtained from Piecewise Logistic Map over Integers

*Sota Eguchi, Takeru Miyazaki, Shunsuke Araki, Satoshi Uehara, Yasuyuki Nogami*

We have been studying a design of the pseudorandom number generator by generated sequences with the logistic map over integers. Although it has already been presented that such properties of the generation sequences are good, the range of control parameters that satisfy the properties is not enough wide. To improve this problem, Wang et al. proposed the piecewise logistic map. It is method for increasing the range of control parameters that can generate good sequences for the pseudorandom number generator. However, it is not suitable for computer implementation, because it is defined over real numbers. In this paper, we will propose a piecewise logistic map over integers that uses an integer arithmetic and computers can calculate the map correctly. We will also show some results of numerical experiments for the sequences generated from this map.

C04-03

### Almost perfect sequence family with perfect crosscorrelation

*Gangsan Kim, Hong-Yeop Song*

Perfect sequence (PS) is the sequence with zero autocorrelation at all the non-zero phase-shifts and $(M, L)$-almost perfect sequence (APS) is the sequence of period L that has zero autocorrelation except for M non-zero phase-shifts. In this paper, we propose a $((q-1)/d-1, (q^n-1)/d)$-APS family with set size $(q-1)/d-1$ constructed from relative difference sets for prime power $q$ and divisor $d$ of $q-1$. We further prove that the proposed family has perfect crosscorrelation.

C04-04

### A Study on Binary Sequences Located in Hadamard Matrices of Order $2^n$

*Kasumi Nakano, Kako Takahashi, Satoshi Uehara, Takeru Miyazaki, Shunsuke Araki, Yasuyuki Nogami*

We show some properties of binary sequences located in Hadamard matrices of order $2^n$ represented by Sylvester's matrices. The Kronecker product is a method for expanding Hadamard matrix, and a set of sequences with orthogonal properties is extended by concatenation or interleaving. From these expanding methods and properties related to constructions, we discuss the increase of a set of orthogonal sequences. Finally, we show the characteristic polynomials of binary sequences located in Hadamard matrices of order $2^n$.

## Data Privacy and Security

C05-01

### Cache-22: A Highly Deployable Encrypted Cache System

*Keita Emura, Shiho Moriai, Takuma Nakajima, Masato Yoshimi*

Cache systems are crucial for reducing communication overhead on the Internet. The importance of communication privacy is being increasingly and widely recognized; therefore, we anticipate that nearly all end-to-end communication will be encrypted via secure sockets layer/transport layer security (SSL/TLS) in the near future. Herein we consider a catch-22 situation, wherein the cache server checks whether content has been cached or not, i.e., the cache server needs to observe it, thereby violating end-to-end encryption. We avoid this catch-22 situation by proposing an encrypted cache system which we call Cache-22. To maximize its deployability, we avoid heavy, advanced cryptographic tools, and instead base our Cache-22 system purely on traditional SSL/TLS communication. It employs tags for searching, and its design concept enables the service provider to decide, e.g., via an authentication process, whether or not a particular user should be allowed to access particular content. We provide a prototype implementation of the proposed system using the color-based cooperative cache proposed by Nakajima et al. (IEICE Trans. 2017). We also show that the proposed system is efficient and feasible in practice, suggesting that it will be easy to deploy on the Internet.

C05-02

### Score Fusion Method by Neural Network Using GPS and Wi-Fi Log Data

*Katsuya Matsuoka, Mhd Irvan, Ryosuke Kobayashi, Rie Shigetomi Yamaguchi*

Recently, personal authentication has become more important than ever because of authentication vulnerability problems. In cases where extremely high confidentiality is required, multi-factor authentication is used. In this study, we focus on score fusion method, which merges authentication scores of each factor in multi-factor authentication. In conventional score fusion methods, the weight of each factor is fixed. These methods work well when all users have a similar tendency for each factor. However, behavioral authentication is highly dependent on each user's characteristics, and the tendency of which factors have high accuracy may differ greatly among users. There is no score fusion method suitable for such a case where the tendency of each factor is different. We propose a user dependent weighting score fusion method using a neural network. Since our proposed method constructs a simple binary classification network for each user, the weight is personally adjusted for each user. The comparison experiment results show that True Acceptance Rate (TAR) of our proposed method is higher than conventional methods.

C05-03

### Randomized Nested Polar Subcode Constructions for Privacy, Secrecy, and Storage

*Onur Günlü, Peter Trifonov, Muah Kim, Rafael F. Schaefer, Vladimir Sidorenko*

We consider polar subcodes (PSCs), which are polar codes (PCs) with dynamically-frozen symbols, to increase the minimum distance as compared to corresponding PCs. A randomized nested PSC construction with a low-rate PSC and a high-rate PC, is proposed for list and sequential successive cancellation decoders. This code construction aims to perform lossy compression with side information. Nested PSCs are used in the key agreement problem with physical identifiers. Gains in terms of the secret-key vs. storage rate ratio as compared to nested PCs with the same list size are illustrated to show that nested PSCs significantly improve on nested PCs. The performance of the nested PSCs is shown to improve with larger list sizes, which is not the case for nested PCs considered.

C05-04

### Fountain Codes for Private Distributed Matrix-Matrix Multiplication

*Rawad Bitar, Marvin Xhemrishi, Antonia Wachter-Zeh*

We consider the problem of designing codes with flexible rate (referred to as rateless codes) for private distributed matrix-matrix multiplication. A master server owns two private matrices **A** and **B** and wants to hire worker nodes to help compute the multiplication. The matrices should remain private from the workers, in an information-theoretic sense. This problem has been considered in the literature and codes with a predesigned threshold are constructed. More precisely, the master assigns tasks to the workers and waits for a predetermined number of workers to finish their assigned tasks. The size of the tasks assigned to the workers depends on the designed threshold. We are interested in settings where the size of the task must be small and independent of the designed threshold. We design a rateless private matrix-matrix multiplication scheme, called RPM3. Our scheme fixes the size of the tasks and allows the master to send multiple tasks to the workers. The master keeps receiving results until it can decode the multiplication; hence the flexibility of the rate. Two main applications require this property: i) leverage the possible heterogeneity in the system and assign more tasks to workers that are faster; and ii) assign tasks adaptively to account for a possibly time-varying system.

C05-05

### Data Anonymization for Service

### Strategy Development and Information Recommendation to Users Based on TF-IDF Method

*Kazuhiro Kono, Noboru Babaguchi*

This paper proposes a data anonymization method considering service strategies and information recommendations for users. Adopting the TF-IDF method, we attach importance to the personal data attributes required for strategy development and user's information recommendation in the case of anonymization. As a result, we generate anonymized personal data suitable for the strategy and the recommendation. We examine through simulation that the anonymized data generated by our method leaves information required for the recommendation in more detail.

## Network Security and Computer Security

C06-01

### Detection Bottleneck links without multiple nodes

*Hiroomi Isozaki*

A "Link Flooding Attack" is that does not directly attack the target node, but instead creates a state in which packets cannot reach the target node by congestion of the intermediate link. In general, it is best way to distribute multiple measurement nodes to measure the network and monitor the links that are bottlenecks. In this paper, we propose a method to detect a bottleneck link, that is attacked, by a single node, without requiring multiple measurement nodes. Next, we show the effectiveness of our proposal method using a network topology by a topology generator. Finally, we detect links that may be bottleneck links by applying our proposal method to the actual Traceroute data.

C06-02

### A Decentralized Secure Email System based on Conventional RSA Signature

*Kazumasa Omote*

Recently, many users have been attacked by phishing or targeted malicious email, and thus email has become completely untrustworthy. So we gradually need to make email communications more secure. Of course, we can digitally sign, encrypt and decrypt emails by secure email systems such as S/MIME and PGP, which are two standards developed for that purpose. However, these two systems are seldom used and then have some drawbacks: the trust mode of PGP is only suitable for small-scaled organizations, and S/MIME cannot run away from the troubling operations such as the certificate application. In this paper, we propose a decentralized and large-scaled secure email system using conventional RSA signature embedding ID (e.g., email address), which is used in the communication scene among unspecified multi-organization. More importantly, our system needs neither a public key certificate nor voucher (e.g., CA or trusted user) for mail security by employing the new type of "key trust level". Since the reliability of email is decided by user itself rather than is decided by other vouchers, we can say that our system is truly decentralized.

C06-03

### Memory Efficient and Provably Secure Virus Detection

*Hayami Motohashi, Kazuki Yoneyama*

Lipton et al. introduced a provably secure virus detection scheme. However, their scheme needs larger memory than the original program because the program is extended to detect virus injections. In this paper, we introduce a new virus detection scheme which needs smaller memory than Lipton et al.'s scheme. We also prove that our scheme is secure in the same security model of their scheme.

C06-04

### Packer Identification Method for Multi-layer Executables with k-Nearest Neighbor of Entropies

*Omachi Ryuto, Yasuyuki Murakami*

The damage cost caused by malware is increasing in the world. Malware coders usually use the method of packing to hinder malware detection and analysis. It is a hard task even for professional malware analysts to unpack a re-packed or a multi-layer packed malwares Bat-Erdene et al. propose a method to identify a packer of multi-layer packing using SAX. Serdar shows that k-nearest neighbor algorithm is the best method to identify the packer of single-packing among the following 4 algorithms: k-Nearest neighbor, Best-first decision Tree, Sequential minimal optimization and Naive Bayes. It can be considered that k-nearest neighbor algorithm is also effective to identify the packer for multi-layer packed malwares. In this paper, we propose a method to identify the packer for multi-layer packed malwares by using k-nearest neighbor algorithm with entropy-analysis for the malwares.

## Information Hiding

C07-01

### Addressing Information Using Data Hiding for DNA-based Storage Systems

*Takahiro Ota, Akiko Manada*

DNA-based storage systems have been recently studied very well because the systems have ultra-high density and ultra-long endurance compared with traditional data storage media. DNA-based storage systems use a DNA strand which stores a subblock of an input data. Additionally, its infra-file location (an address or index of the subblock) is also stored to restore the input data from a set of DNA strands. In fact, the cost of the indices becomes large as input data size goes to large. Moreover, the cost of constructing DNA strands, called synthesizing, is expensive. In this paper, for reducing the cost of indices in DNA strands, we propose addressing information using data hiding (steganography) for DNA-based storage systems. The proposed algorithms embed an index to a subblock of an input data in a DNA strand, and the index block is removed from a DNA strand. We also evaluate the number of bits which can be embed to a subblock for variants of conventional DNA-based storage systems. The scheme of the proposed algorithm can be applied to embed not only addressing information but also some valuable information such as a summary and the copyright of the file to DNA strands.

C07-02

### Visible Video Data Hiding Techniques Based on Visual Effects Utilizing Barcodes

*Tetsuya Kojima, Kento Akimoto*

Data hiding techniques are usually applied into digital watermarking or digital fingerprinting, which is used to protect intellectual property rights or to avoid illegal copies of the original works. It is pointed out that data hiding can be utilized as a communication medium. It is required that the difference between the cover objects and the stego objects are quite small in order that the difference cannot be recognized by human sensory systems. On the other hand, the authors have proposed a hearable data hiding technique for audio signals that can carry secret message and can be naturally recognized as a musical piece by human ears. In this study, we extend the idea of the hearable data hiding into video signals by utilizing the visual effects. As visual effects, we employ fade-in and fade-out effects which can be used as a kind of visual rendering for scene transitions. In the proposed schemes, secret messages are generated as one-dimensional barcodes which are used for fade-in or fade-out effects. The present paper shows that the proposed schemes have the high accuracy in extracting the embedded messages even from the video signals captured by smartphones. It is also shown that the video signals conveying the embedded messages can be naturally recognized by human visual systems through subjective evaluation experiments.

## Wireless Communications

D01-01

### Multi-Carrier Differential Trellis-Coded Modulation/Demodulation Employing Multiple Differential Detection with Channel Prediction

*Tetsuro Kubo, Hiroshi Kubo*

This paper proposes a multi-carrier (MC) modulation scheme employing differential trellis-coded modulation (DTCM) and multiple differential detection with channel prediction in order to cope with doubly-selective fading at the good required signal-to-noise power ratio (SNR), where doubly-selective channels correspond to severe time/frequency-selective channels. For frequency-selective fading, MC modulation schemes are effective. For time-selective fading, multiple differential detection employing per-survivor processing (PSP-MDD) with channel prediction is effective. However, channel prediction degrades the required SNR for PSP-MDD. In order to cope with doubly-selective fading and improve the required SNR, this paper proposes MC-DTCM employing PSP-MDD with channel prediction. Finally, computer simulation results show that the proposed scheme can improve both the performance for doubly-selective fading and the required SNR compared with the conventional PSP-MDD with channel prediction.

D01-02

### Improvement of accuracy of UWB Positioning System within the intersection using a Long Short-Term Memory Network

*Yuki Noda, Shunya Asano, Makoto Itami, Akira Nakamura*

In this paper the pedestrian positioning system in the intersection using UWB(Ultra-Wide Band) is studied. In this system, UWB signal is transmitted from the terminal owned by each pedestrian and it is received by base stations attached to traffic lights for pedestrian, and the distance to the pedestrian is measured. Distance between the pedestrian and the base station is estimated by TOA (Time Of Arrival) of the received signal. The position of the pedestrian is estimated by LSM (Least Square Method) using the distance measurement value. The accuracy of UWB positioning system deteriorates due to thermal noise and multipath. The distribution of this accuracy differs for each position, and it is complicated to create a mathematical model to correct. In this paper, appropriate correction is performed by learning different noise distributions for each position using LSTM (Long Short-Term Memory), a kind of RNN (Recurrent Neural Network). In addition, we propose a network that estimates the current value using previous observations in order to estimate the position even if the positioning of the pedestrian fails. The effectiveness of the proposed method is verified by comparing the performance with positioning using the Kalman filter. As a result of computer simulation, it is shown that the proposed method achieves high accuracy positioning performance.

D01-03

### On an Alternative Approach to Congestion Detection in Ad Hoc Networks

*Xiaojie Liu, Ulrich Speidel*

Ad hoc wireless networks without pre-existing infrastructure depend on mutual collaboration among nodes. Congestion in such networks presents more of a challenge than in other types of networks. An essential task in this context is to determine when a node is congested. This paper considers the use of T-entropy to detect network congestion, and in particular how to define an appropriate entropy threshold for congestion detection. The paper first discusses how to recognise a congested node from the perspective of (one of) its neighbours. We then simulate ad hoc network scenarios, which we analyse for goodput and entropy to determine the relationship between entropy and the network congestion situation. As its main result, this paper proposes an entropy threshold algorithm for congestion detection in these scenarios for use in an AODV (Ad hoc On-Demand Distance Vector Routing) derivate, RAODV (Relieving AODV), that uses uncongested neighbours to detect and relieve congestion.

D01-04

### Optimal Power Allocation of Cooperative Superposition-Coded Relaying with Finite-Blocklength Transmission over Quasi-Static Rayleigh Channels

*Masaya Kambara, Guanghui Song, Tomotaka Kimura, Jun Cheng*

Analytic performance of cooperative superposition-coded relaying systems over quasi-state Rayleigh channels with finite-blocklength transmission is given. The CDF of SINR of maximum ratio combining signal in the receiver is derived, and a closed-form representation of the corresponding outage probability is given. Moreover, the transmission powers are optimized analytically such that the normalized system throughput is maximum.

D01-05

### Latency-Energy Tradeoff with Realistic Hardware Models

*Anders Høst-Madsen, Nicholas Whitcomb, Jeffrey Weldon, Zixiang Xiong*

Latency and energy are two fundamental parameters that characterize communications systems performance. In this paper we investigate the fundamental relationship between these quantities using finite blocklengh information theory. We take into account realistic models of hardware, including overhead power, power amplifier inefficiency and the receiver noise factor. With these models we find that energy and latency behaves quite different from the ideal case.

D01-06

### Study on a delay and Doppler estimation performance of 2-dimensional BPSK signal using discrete gaussian wave

*Masayoshi Ohashi*

Precise estimation of delay $t_d$ and Doppler $f_D$ associated with wireless transmission is a basic problem of radar technology, as well as synchronization and channel estimation for wireless communications. The author has been studying an estimation method using 2-dimensional BPSK signal. It was originally proposed by Kohda and Jitsumatsu and its performance was evaluated with continuous signal model. Recently Kohda has remodeled this scheme into the discrete model, the author reports its performance characteristics.

## Signal Processing

D02-01

### Deep Convolutional Autoencoders for Deblurring and Denoising Low-Resolution Images

*Michael Fernando Mendez Jimenez, Omar DeGuchy, Roummel Marcia*

In this paper, we implement machine learning methods to recover higher-dimensional signals from lower- dimensional, noisy, and blurry measurements. In particular, rather than utilizing optimization-based reconstruction methods, we use fully-connected multilayer perceptron (MLP) architectures and convolutional neural networks (CNN). In addition, we consider two different loss functions based on mean squared error and a Huber potential to train our models. Numerical experiments on the Street View House Numbers dataset show that while fully-connected MLPs are faster to train, reconstructions using CNNs are much more accurate.

## Acoustic Communications

D03-01

### Experimental Evaluation Results of Acoustic Spread Spectrum Communications Employing Orthogonal Gold Sequences

*Haruka Toyota, Hiroshi Kubo*

This paper proposes code division multiple access (CDMA) acoustic spread spectrum communications for uplink terrestrial acoustic communications. For CDMA, the multiple access performance strongly depends on the auto/cross-correlation of the spreading codes. Therefore, this paper discusses a spreading code search criterion based on the orthogonal Gold sequences, which can select a set of spreading codes with good auto/cross-correlation at small computational complexity. Next, this paper proposes a frame structure, synchronization schemes, and frequency response of band-pass filters to cope with acoustic ambient noises, for the proposed acoustic spread spectrum communications. Finally, field evaluation results confirm that the proposed acoustic spread spectrum communications have good performance thanks to the proposed band-pass filter.

D03-02

### Differential OFDM Employing AFC for Fast Time-Varying Doppler Shifts in Underwater Acoustic Communications

*Yui Nakai, Yuka Tanaka, Hiroshi Kubo*

This paper proposes differential orthogonal frequency division multiplexing (OFDM) employing automatic frequency control (AFC) for fast time-varying Doppler shifts in underwater acoustic communications (UWACs). There exist the following two problems in UWACs: 1) severe time and frequency selectivities, i.e., double selectivity; 2) fast time-varying Doppler shifts. With respect to the problem 1), the proposed scheme employs differential encoding/differential detection (DE/DD) for time selectivity, and it also employs OFDM for frequency selectivity. With respect to the problem 2), the proposed scheme employs a multiple open-loop frequency estimation (MOLFE), which has a good tradeoff between frequency coverage and estimation accuracy in a short observation time. Next, this paper proposes a simple time-varying Doppler shift simulation model for autonomous underwater vehicle (AUV) turning. Finally, computer simulation results confirm that the proposed differential OFDM employing MOLFE has excellent performance in doubly-selective channels with fast time-varying Doppler shifts.

D03-03

### Doubly Differential OFDM Employing an Intercarrier Interference Self-Canceller for Underwater Acoustic Communications

*Yuka Tanaka, Yui Nakai, Hiroshi Kubo*

This paper proposes doubly differential orthogonal frequency division multiplexing (OFDM) for underwater acoustic communications (UWACs) in the presence of large

Doppler shifts. UWAC channels suffer from severe time and frequency selectivities, i.e., double selectivity. OFDM is a good solution for frequency selectivity, and differential encoding/differential detection (DE/DD) is a good solution for time selectivity. DE/DD can cope with time selectivity without insertion of pilot-symbol. However, OFDM suffers from intercarrier interference (ICI) due to its narrow subcarrier spacing. Although an intercarrier interference self-canceller (ICISC) can cancel ICI for differential OFDM, DE/DD cannot cope with severe time-selective channels. In order to solve these issues, this paper proposes doubly differential OFDM employing the ICISC for severe doubly-selective channels. Finally, computer simulation results confirm that the proposed doubly differential OFDM has excellent performance on UWAC channels.

D03-04

### Designing a Symbol Classifier for Inaudible Sound Communication Systems Using a Neural Network

*Kosei Ozeki, Naofumi Aoki, Saki Anazawa, Yoshinori Dobashi, Kenichi Ikeda, Hiroshi Yasuda*

This study has developed a system that performs data communications using high frequency inaudible band of sound signals. Unlike radio communication systems using specified wireless devices, it only requires microphones and speakers employed in ordinary telephony communication systems. In this study, we investigate the possibility of a machine learning approach to improve the recognition accuracy identifying binary symbols transmitted through sound signals. This paper describes some experiments evaluating the performance of our proposed technique employing a neural network as its classifier. The experimental results indicate that the proposed technique may have certain appropriateness for designing an optimal classifier for the symbol identification.

## Statistical Inference and Learning

E01-01

### Asymmetry models and model selection in square contingency tables with ordinal categories

*Kouji Tahata, Tatsuya Ochiai, Ukyo Matsushima*

Various types of asymmetry models have been proposed to analyze square contingency tables with ordinal categories. Here, we show that each of these models can be interpreted as a property that it is the closest to the symmetry model in terms of the Kullback-Leibler divergence under some conditions. The relationship between the likelihood ratio chi-square statistic for symmetry and that for asymmetry is discussed. Additionally, an asymmetry model family is given, and models included in it are referred to as nonhierarchical models. Because it is difficult to compare two asymmetric models, we treat this as a model selection problem. To address, we employ the penalized likelihood approach and conduct simulation studies.

E01-02

### Statistical Testing of Randomness

*Boris Ryabko*

The problem of constructing effective statistical tests for random sequences of binary digits is considered. The effectiveness of such statistical tests is mainly estimated on the basis of experiments with various random number generators. We consider this problem in the framework of mathematical statistics and find an asymptotic estimate for the p-value of the optimal test in the case when the alternative hypothesis is an unknown stationary ergodic source.

E01-03

### Optimal Resolution of Change-Point Detection with Empirically Observed Statistics and Erasures

*Haiyun He, Qiaosheng Zhang, Vincent Y. F. Tan*

This paper revisits the offline change-point detection problem from a statistical learning perspective. Instead of assuming that the underlying pre- and post-change distributions are known, it is assumed that we have partial knowledge of these distributions based on empirically observed statistics in the form of training sequences. Using the training sequences as well as the test sequence consisting of a single-change and allowing for the erasure or rejection option, we derive the optimal resolution between the estimated and true change-points under two different asymptotic regimes on the undetected error probability—namely, the large and moderate deviations regimes. In both regimes, strong converses are also proved. In the moderate deviations case, the optimal resolution is a simple function of a symmetrized version of the chi-square distance.

E01-04

### On MDL Estimation for Simple Contaminated Gaussian Location Families

*K. Miyamoto, Junichi Takeuchi*

The performance of MDL density estimators defined as the minimizer of two part code lengths is guaranteed in terms of the redundancy of the two part code [2], [3]. When the true density belongs to the assumed model, the redundancy of a code can be bounded by the regret (pointwise redundancy) of the code. Then, the construction of two part codes which achieve small regret based on quantization of parametric family is developed. For exponential families, it is known that we can achieve sufficiently small regret by using this construction [4]. For non-exponential families, the evaluation of the regret achieved by using this construction breaks. However, for nonexponential families under certain assumptions, by enhancing this construction using local exponentially family bundles [1], we can design efficient two part codes [9]. In this paper, we show that we can apply this coding method to contamination model [5] with simple settings and give the guarantee of performance of MDL estimators for them.

## Machine Learning and Information Theory

E02-01

### Differential Description Length for Hyperparameter Selection in Supervised Learning

*Mojtaba Abolfazli, Anders Høst-Madsen, June Zhang*

Minimum description length (MDL) is an established method for model selection. For supervised learning problems, cross-validation is often used for model selection in practice. Reasons are 1) MDL is difficult to apply directly to data; 2) MDL may make restrictive statistical assumptions that decrease performance; and 3) MDL does not directly aim to minimize generalization error. In this paper, we introduce a modification to MDL, which we call differential description length (DDL). DDL partitions the data so that the codelength(s) it computes, reflects the conditional probability of seeing 'new' data given 'old' data. This differential codelength is what allows DDL to estimate generalization error like cross-validation. DDL is also better than cross-validation because it allows the learning algorithm to use the entire data without having to withhold subsets for validation and testing. Compared with MDL, DDL has both better performance (in finding models with smaller generalization error) and is easier to compute. Experiments with linear regression and deep neural networks show that DDL also outperforms cross-validation.

## Formalization

E03-01

### Formalization of VT Codes and Their Single-Deletion Correcting Property in Lean

*Yuki Kondo, Manabu Hagiwara, Midori Kudo*

This manuscript reports on our project on formalization for deletion codes in Lean theorem prover: the definition of Varshamov-Tenengolts (VT) codes and their single-deletion error-correcting property are formalized. It also reports progress on our attempt to resolve an open problem of VT codes in Lean.

E03-02

### Formal Verification of Merkle-Damgård Construction in ProVerif

*Mieno Takehiko, Yoshimura Togo, Hiroyuki Okazaki, Yuichi Futa, Kenichi Arai*

ProVerif is one of the most successful automatic cryptographic protocol verifiers. However, in ProVerif, it is difficult to formalize recursive execution, whose internal state is changed by an execution result, such as a stream cipher. In this paper, we propose a method of formalizing recursive execution with an internal state in ProVerif. In our proposed method, we treat function calls as communication between internal processes using private channel. The Merkle-Damgård construction (MD construction) is a method of constructing a cryptographic hash function such as SHA-1 or MD5. The behavior of MD construction is similar to recursive execution, because its construction includes one-way compression functions and an internal variable changed by the output of these functions. We also formalize the MD construction algorithm utilizing our proposed method for recursive execution. We verify that our formal model of MD construction successfully holds properties of cryptographic hash function, preimage resistance and collision resistance.

E03-03

### Formal Verification and Code-Generation of Mersenne-Twister Algorithm

*Takafumi Saikawa, Kazunari Tanaka, Kensaku Tanaka*

We formalize the pseudocode and linear-algebraic presentations of Mersenne-Twister, and formally establish their equivalence. Based on this formalization, we investigate the long-period property of Mersenne-Twister, formally proving that the property is reduced to the primitivity of the characteristic polynomial of the matrix representation. The formalization is done in Coq proof assistant. This enables us to generate a C program code from the verified pseudocode written in Coq .

**Author Index**

SITA
Since 1978