情報理論基礎応用研究ステーション
研究成果報告書

平成14年～平成18年度

代表者名　　小林　欣吾

研究ステーション研究成果報告書

１．研究ステーション名　　情報理論基礎応用研究ステーション

２．設置期間　　平成１４年～平成１８年度

３．代表者名　　小林　欣吾

４．研究ステーションとしての活動概要

情報理論基礎応用研究ステーションは平成 14 年(2002 年)に学内外の関連する研究者を結集して立ち上げ，情報通信の理論と応用に関わる研究の活性化を目指してきた。 その主要なテーマを、国際的な連携と国際的な舞台で活躍できる若手研究者の育成においている。

本ステーションの前身は 1970 年代中葉、本学名誉教授佐藤洋先生が中心となり、東京地区の若手情報理論研究者が自発的に参加して形成された「情報と符号研究会」（略称Ｉ＆Ｃ研究会）である。 その事務局としての役割を電気通信大学のメンバーが担う事が多かった。 これまで、定期的、あるいは不定期にセミナーをわが大学にて開催し、ときには他大学に開催場所を移して、容赦のない批判と熱のこもった激論を交わしながら切磋琢磨して各メンバーが成長を遂げる場としてきた。 海外の情報理論研究者の多くが日本を訪れるときには、このセミナーで最新の話題を提供していくということが普通に行われるようになっていた。この伝統は本研究ステーションに引き継がれている。

1949 年の本学開学にあたり、初代学長寺沢寛一先生が米国において画期的な通信の新理論が、一人の天才（Claude E. Shannon）によって生み出されたということにいち早く気付かれて、電気通信大学の基礎を支えるものとしてその理論を確実に習得し研究を怠らない様にと佐藤洋先生らを指導されたという経緯がある。その意志を体現しようとされた佐藤洋先生の心意気に惹かれて参加した古参のＩ＆Ｃのメンバーばかりでなく、学内外の優秀な若手研究者を加えて、この分野の研究のさらなる深化と新たな展開を計ることを目的として、平成１４年度に研究ステーションとしての活動を始め，情報理論の未解決問題，マルチユーザ情報理論，ネットワーク情報理論，情報スペクトル理論，量子情報理論，情報セキュリティー，乱数生成，データ圧縮，符号化・復号化，高速アルゴリズムなどの理論的研究を行っている。 また、注目されるテーマに関しては、関係する学会（情報理論とその応用学会(SITA)、電子情報通信学会情報理論研究専門委員会(IEICE-IT)、IEEE IT Society Japan Chapter など）との連携のもとにワークショップ企画も計画・実施して成果に結び付けている。 さらに、米国 UCSD の「情報理論と応用研究センター（Center for Information

Theory and Applications）」との関係を強化し、また、アジア・ヨーロッパ情報理論ワークショップの持続的開催を支えて、ヨーロッパの研究者との連携を深めることにより研究活性化を行っている。特記されることは、平成 15 年 IEEE International Symposium on Information Theory, Yokohama の直前に、本研究ステーションが文科省の国際シンポジウム開催経費の援助ならびに本学の補助を受けて、千葉鴨川において主催した国際ワークショップは、情報理論の中核的な研究者が、国内、海外バランスよく参加して極めてレベルの高い研究交流の場を提供したことである。

こうした動きに伴い、平成 15 年鴨川ワークショップ以来、米国 UCSD との関係が密接になってきている。UCSD は、CALIT2 (California Institute for Telecommunication and Information Technology)の中心的大学として位置しており、その理論的中核を形成するのが、平成 18 年 2 月に UCSD に設立された「情報理論と応用研究センター（Center for Information Theory and Applications)」である。そのセンターの開所 ITA ワークショップには世界から気鋭の研究者 500 名ほどが参加し、1週間にわたってパラレル 3 セッションで熱気のある研究発表が行われた。本年 1 月にも第 2 回の ITA ワークショップが開催され、550 名ほどの参加者がパラレル 5 セッションで研究発表が行なわれた。UCSD の CITA の指導的立場にある Jack K. Wolf 教授のもとで薫陶を受けた Brian Kurkosky 氏はこの 3 月より情報通信工学科の助教授に着任し、研究ステーションのメンバーとしての活躍も期待されている。UCSD の CITA と我々の研究ステーションの連携は互いの研究活動に多大の刺激を与えると考えられる。

またヨーロッパでは伝統的に情報理論の基礎研究を重視している。アイントホーフェン工科大学、エッセン工科大学、ビーレフェルト大学は重要な位置を占めるがこれらとも我々の研究ステーションのメンバーは深い関係を有し、実際、日本・ベネルックス情報理論ワークショップを継承したアジア・ヨーロッパ情報理論ワークショップを連携を保ちながら8回にわたる開催を主導してきた。さらに、近年では、米国から帰国して香港大学に拠点を構える Yeoug 教授、Feng 教授らの研究者グループ、西安の Cai 教授らとの関係ではネットワーク符号化を中心に研究交流が加速することが期待されている。

平成 14-15 年は IEEE International Symposium on Information Theory, Yokohama のプログラム委員会の共同委員長として韓太舜教授、阪田省二郎教授があたり、さらに、研究ステーションのメンバーが数人、委員として加わり、シンポジウムの中核として活動した。このシンポジウムにおいて、本ステーションのメンバーである長岡助教授は、大会のハイライトである Plenary Lecture の講演を行い、量子情報理論の現状と展望を解説し、多くの聴衆に感銘を与えた。ステーション発足以前には、韓太舜教授は平成 12-13 年に情報理論とその応用学会会長を務めており、小林欣吾教授は平成 16～17 年にわたって、情報理論とその応用学会会長を務め、また、平成 19 年度には電子情報通信学会基礎境界ソサイエティーの次期会長となる。さらに、彼は平成 16 年以来、IEEE Transactions on Information Theory の Shannon Theory の Associate Editor,Award Committee の一員として国際的な情報理論研究の発展に貢献している。なお、本ステーションには、IEEE のフェ

ローが4名（韓、阪田、小林、藤野）、電子情報通信学会フェローが 3 名（韓、阪田、小林）存在している。

5．研究ステーションとしての活動状況

●主な講演会、シンポジウム等の開催状況等：

以下の研究セミナーを学術講演会，IS セミナー，研究室セミナーとして情報理論基礎応用研究ステーションが主催，共催などの形をとって行った．

日時：平成 14 年 7 月 19 日（金）15:00~16:30
講演者： Hosam M. Mahmoud(Professor, The George Washington University)
演題: Probabilistic analysis of Random Trees via Urn Models

日時：平成 15 年 7 月 7 日（月）15:00~16:30
講演者： Jack K. Wolf(Professor, University of California San Diego)
演題: Bit Stuffing for Protocols and Constrained Systems

日時：平成 15 年 7 月 7 日（月）16:30~18:00
講演者： A. J. Han Vinck(Professor, Universitaet Essen)
演題: On Security Aspects for Critical Infrastructures

日時：平成 16 年4月6日（火）
講演者： Raymond Yeung (Professor, National University of Hong Kong)
演題 1: Information Inequalities, Conditional Independence, and Groups
演題 2: Network Coding Theory

日時：平成 16 年4月 19 日（月）
講演者： Vladimir I. Levenshtein (Professor, Keldysh Institute for Applied Mathematics, Russian Academy of Sciences)
演題: Combinatorial and probabilistic problems of sequence reconstruction

日時：平成 16 年 7 月 7 日（月）10:40~12:10
講演者： Tom Hoeholdt(Professor, Technical University of Denmark)
演題: List decoding of Reed-Solomon codes

日時:平成 16 年 8 月 10 日(火)
講演者: Dr. Brian Kurkoski (University of Electro-Communications)
演題: Sequence ML and Symbol MAP Decoding on the Erasure Channel

日時:平成 16 年 8 月 10 日(火)
講演者: Marc Fossorier (Professor, University of Hawaii)
演題: Simplifications of BP decoding of LDPC codes

日時:平成 16 年 9 月 24 日(金)
講演者: Ken Zeger (Professor, Department of Electrical and
Computer Engineering, University of California, San Diego)
演題1: Network Coding - Linearity and Solvability
演題2: Asymptotics of Run-Length Constraints for Hexagonal Lattices

日時 : 平成 16 年 11 月 12 日(金)
講演者: Hosam M. Mahmoud (Professor, The George Washington University)
講演題目: Polya process and random sprouts

日時 : 平成 17 年 4 月 14 日(木)16:00~18:00
講演者: Paul H. Siegel (Professor, Department of Electrical and Computer Engineering,
University of California, San Diego)
題目: Constrained Coding Techniques for Advanced Data Storage
Devices

日時 : 平成 17 年 10 月 4 日(火) 9:00 ～ 10:00
講演者: Taraz, Anusch (Professor, ドイツ・ミュンヘン工科大学数学科)
題目 : Large planar subgraphs in dense graphs

日時 : 平成 17 年 11 月 11 日(金)15:00～17:00
講演者: Marat Burnashev (Professor, Russian Academy of Sciences)
題目 : On Some Singularities in Parameter Estimation Problems

日時 : 平成 18 年 3 月 17 日(金) 15:30 ～ 17:00
講演者: 玉城史朗(琉球大学工学部教授)
題目 : 「閾値秘密分散法に基づくネットワークストレージ法に関する研究」

日時 ： 平成 18 年 8 月 10 日(木) 17:00 ～ 18:00
講演者： Andrea Goldsmith (Assoc. Prof., Stanford University, Department of Electrical Engineering)
題目 ： Capacity, cooperation, and cross-layer design in wireless networks

日時 ： 平成 18 年 9 月 6 日(水) 16:30 ～ 18:00
講演者： Ken Zeger (Professor, University of California, San Diego)
題目 ： Matroids, Networks, and Non-Shannon Information Inequalities

日時 ： 平成 19 年 1 月 16 日(水) 14:30 ～ 16:10
講演者： 朴 英蘭 （特別研究員）
題目 ： An introduction of pixel based steganographic methods endenumerate

●代表的なピアレビュー論文発表、学会プレナリ、招待講演発表、特許出願、受賞等

ピアレビュー論文発表

[1] M.Iwamoto and H.Yamamoto, ``The optimal n-out-of-n visual secret sharing scheme for gray-scale images,'' IEICE Trans. on Fundamentals, vol.E85.A, no.10, pp.2238-2247, Oct. 2002.

[2] Akiyama, Jin; Ando, Kiyoshi; Egawa, Yoshimi, ``Graph G for which both G and $ bar G$ are contraction critically$k$-connected,'' Graphs Combin. 18 (2002), no. 4, 693--708.

[3] Ando, Kiyoshi; Nakamoto, Atsuhiro,``Self-complementary graphs with minimum degree two,''
Ars Combin. 65 (2002), 65--74

[4] Kojima, Toru; Ando, Kiyoshi; Kaneko, Atsushi,``Edge-wide-diameter of graphs with diameter d,''Ann. Comb. 6 (2002), no. 1, 57--64.

[5] Ando, Kiyoshi; Kaneko, Atsushi; Kawarabayashi, Ken-ichi; Yoshiomoto,Kiyoshi,``Contractible edges and bowties in a k-connected graph, ''Ars Combin. 64 (2002), 239--247.

[6] Kojima, Toru; Ando, Kiyoshi,``Bandwidth of the Cartesian product of two connected graphs,"
Discrete Math. 252 (2002), no. 1-3, 227--235.

[7] Ando, Kiyoshi; Nakamoto, Atsuhiro,``On quadrangulations of closed surfaces covered by vertices ofdegree 3,"Ars Combin. 62 (2002), 121--127.

[8] Ando, Kiyoshi; Egawa, Yoshimi; Kaneko, Atsushi; Kawarabayashi, Ken-ichi; Matsuda, Haruhide,``Path factors in claw-free graphs,"Discrete Math. 243 (2002), no. 1-3, 195--200.

[9] H. Kostadinov, H. Morita, N. Manev, ``Integer Codes Correcting Single Errors of Specific Types $(pm e1, pm e2, ldots, pm e_s)$, " IEICE Trans. Fundamentals, E86-A, 7, pp.1843--1849, 2003.

[10] M.Iwamoto and H.Yamamoto, ``A construction method of visual secret sharing schemes for plural secret images," IEICE Trans. on Fundamentals, vol.E86.A, no.10, pp.2577-2588, Oct. 2003.

[11] Ando, Kiyoshi; Kaneko, Atsushi; Kawarabayashi, Ken-ichi,``Vertices of degree 6 in a contraction critically 6-connected graph,"Discrete Math. 273 (2003), no. 1-3, 55--69.

[12] Ando, Kiyoshi; Kawarabayashi, Ken ichi,``Some forbidden subgraph conditions for a graph to have a k-contractible edge,"Discrete Math. 267 (2003), no. 1-3, 3--11.

[13] Ando, Kiyoshi; Egawa, Yoshimi,``Maximum number of edges in a critically k-connected graph,"
Discrete Math. 260 (2003), no. 1-3, 1—25

[14] Hristo Kostadinov, Hiroyoshi Morita, Nikolai Manev, ``Derivation on Bit Error Probability of Coded QAM using Integer Codes," IEICE Trans. Fundamentals, E87-A, 12, pp.3397--3403, 2004.

[15] 太田 隆博, 森田 啓義, ``反辞書を用いた心電図の1パス無ひずみ圧縮," 電子通信学会論文誌(A), J87-A, 9,pp.1187--1195, 2004.

[16] Yuichi Komano, Kazuo Ohta, ``OAEP-ES -Methodology of Universal Padding Technique-," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, No.1, pp. 110-119, 2004.

[17] Kei Kawauchi, Yuichi Komano, Kazuo Ohta and Mitsuru Tada, ``Probabilistic Multi-Signature Schemes using a One-Way Trapdoor Permutation,'' IEICE Transactions on Fundamentals, vol.E87-A, No.5, pp. 1141-1153, 2004.

[18] T.S.Han, ``Folklore in source coding: information-spectrum-approach, '' IEEE Trans. on Inform. Theory, vol.51, no.2, pp.747-753, 2005.

[19] Hajime Matsui, Syojiro Sakata, Msazumi Kurihara, Seiichi Mita, ``Systolic array architecture implementing Berlekamp-Massey-Sakata algorithm for decoding codes on a class of algebraic curves,'' IEEE Trans. on Information Theory, Vol.51, No.11, pp.3856-3871, 2005.

[20] Hajime Matsui, Shojiro Sakata and Masazumi Kurihara, ``Fast parallel decoding on systolic array architecture for codes on an class of algebraic curves,'' Kokyuroku, RIMS, Kyoto Univ., Vol. 1420 , pp.183－205, 2005.

[21] 木村,大西,小早川,星,大森,``任意の Lp 距離による検索を可能とす る距離変換規則,'' 情報処理学会論文誌・データベース, Vol. 46, No. SIG 8 (TOD26), pp. 93--105, 2005.

[22] Michihiro Kobayakawa, Mamoru Hoshi, and Kensuke Onishi, ``A Method for retrieving music data with different bit rates using MPEG-4 TwinVQ Audio Compression,'' Proc. of ACM Multimedia (MM2005), pp. 459--462, 2005.

[23] M. M. Rashid, T. Kawabata, ``Theoretical Analysis of a Zero-redundancy Estimator with a Finite Window for a Markovian Source,'' IEICE Transactions on Fundamentals, E88-A, pp.2819-2825, 2005.

[24] 長岡浩司,「量子情報幾何の世界」(招待論文), 電子情報通信学会論文誌 vol.J88-A, No.8, pp.874-885, 2005.

[25] 青木真吾,森田啓義,荒俣吉壮,西新幹彦, ``マクロブロックタイプを用いた MPEG2 圧縮動画像のカット点検出,'' 情報処理学会論文誌:コンピュータビジョンとイメージメディア vol. 46, no. SIG15, pp. 51-58, 2005.

[26] Shuji Kawasaki, Hiroyoshi Morita, ``On optimal scale upper bound in wavelet-based estimation for hurst index of fractional Brownian motion,'' Journal of Interdisciplinary Mathematics, vol. 8, no. 2, pp. 195-214, 2005.

[27] Ken-ichi Iwata, Yasutada Oohama, ``Information-Spectrum Characterization of Broadcast Channel with General Source,'' IEICE Trans. Fundamentals, E88-A, 10, pp.2808-2818, 2005.

[28] Ken-ichi Iwata, Yasutada Oohama, ``Information-Spectrum Characterization of Multiple-Access Channels with Correlated Sources,'' IEICE Trans.Fundamentals, E88-A, 11, pp. 3196-3202, 2005.

[29] Dongzhao Sun, Mikihiko Nishaira, Hiroyoshi Morita, ``On Multiple Smoothed Transmission of MPEG Video Streams,'' IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.10, pp.2844-2851, 2005.

[30] T. Fukuda, N. Kanayama and K. Komatsu, ``Prime divisors of special values of theta functions in the ray class field of a certain quadratic field modulo 2^n,'' to appear in Math. Proc. of Cambridge Philosophical Society.

[31] 大久保誠也,西野哲朗,太田和夫,國廣昇, ``Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数について, '' 情報処理学会論文誌:数理モデル化と応用, Vol. 46, No. SIG17(TOM13), pp. 10-19, 2005.

[32] 大久保誠也,西野哲朗,太田和夫,國廣昇, ``物理的実現可能性に優れた量子探索アルゴリズム, '' 情報処理学会論文誌, Vol. 46, No. 6, pp.1416-1425, 2005.

[33] Yasuhiro Takahashi and Noboru Kunihiro, ``A Linear-size Quantum Circuit for Addition with no Ancillary Qubits,'' Quantum Information and Computation, Vol.5 No.6, pp.440-448, 2005.

[34] Brian Kurkoski, Paul Siegel, Jack Wolf, ``Soft-output Detector for Partial-Response Channels Using Vector Quantization,'' IEEE Transactions on Magnetics, vol. 41, no. 10, pp. 2989-2991, October 2005.

[35] Hyun-Ho Kang, Brian Kurkoski, Young-Ran Park, Hye-Joo Lee, Sang-Uk Shin, Kazuhiko Yamaguchi, Kingo Kobayashi, ``Video Fingerprinting System using Wavelets and Error Correcting Codes,'' Lecture Notes in Computer Science, Vol. 3786, pp. 150-164, Springer-Verlag, 2005.

[36] Kiyoshi Ando, Kiyoshi, Atsushi Kaneko, Ken-ichi Kawarabayashi, ``Vertices of degree 5 in a contraction critically 5-connected graph,'' Graphs Combin. 21, no. 1, 27--37, 2005.

[37] Kiyoshi Ando, ``Trivially noncontractible edges in a contraction critically 5- connected graph,'' Discrete Math. 293, no. 1-3, 61--72, 2005.

[38] A.T.Le, X.N.Tran, T.Fujino, ``Combined ML and MMSE multiuser detecter for STBC-OFDM system,'' IEICE Tran. Fundamentals, Vol. E88-A, no. 10, 2915-2925, Oct. 2005.

[39] X.N.Tran, A.T.Le, T.Fujino, ``Combined MMSE-SIC mutiuser detection for STBC-OFDM system,'' IEICE Tran. Commun., Vol. 89-B, no. 5, 280-283, May, 2005.

[40] X.N.Tran, T.Fujino and Y.Karasawa, ``An MMSE detector for multiuser space-time block coded OFDM,'' IEICE Tran. Commun. Vol. E88-B, no. 1, pp. 141-149, Jan. 2005.

[41] 青木真吾, 森田啓義, 荒俣吉壮, 西新幹彦, ``マクロブロックタイプを用いた MPEG2 圧縮動画像のカット点検出,'' 情報処理学会論文誌:コンピュータビジョンとイメージメディア, 46, SIG15, pp.51-58, 2005.

[42] Dongzhao Sun, Mikihiko Nishiara, Hiroyoshi Morita, ``On Multiple Smoothed Transmission of MPEG Video Streams,'' IEICE Trans. Fundamentals, E88-A, 10, pp.2844--2851, 2005.

[43] Shuji Kawasaki, Hiroyoshi Morita, ``On optimal scale upper bound in wavelet-based estimation for hurst index of fractional Brownian motion,'' Journal of Interdisciplinary Mathematics, 8, 2, pp.195--214, 2005.

[44] T. Ogawa, A. Sasaki, M.Iwamoto, and H.Yamamoto, ``Quantum Secret Sharing Schemes and Reversibility of Quantum Operations,'' Physical Review A 72, 032318, 2005.

[45] Norio ADACHI, Satoshi AOKI, Yuichi KOMANO, Kazuo Ohta, ``Solutions to the Security Problems of Rivest and Shamir's Pay Word Scheme,'' IEICE Transactions on Fundamentals, vol.E88-A, No.1, pp. 195-202, May 2005.

[46] Noboru Kunihiro, ``Exact Analyses of Computational Time for Factoring in Quantum Computers,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E88-A, No.1, pp. 105-111, 2005.

[47] 大久保誠也, 西野哲朗, 太田和夫, 國廣昇, ``物理的実現可能性に優れた量子探索アルゴリズム,'' 情報処理学会論文誌, Vol. 46, No.6, pp. 1416-1425, 2005

[48] Yasuhiro Takahashi and Noboru Kunihiro, ``A LINEAR-SIZE QUANTUMCIRCUIT FOR ADDITION WITH NO ANCILLARY QUBITS,'' Quantum Information and Computation, Vol.5, No.6, pp.440-448, 2005

[49] 大久保誠也, 西野哲朗, 太田和夫, 國廣昇, ``Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数について,"情報処理学会論文誌:数理モデル化と応用, Vol. 46, No. SIG17(TOM13), pp. 10-19, 2005

[50] Ando, Kiyoshi, ``Trivially noncontractible edges in a contraction critically 5-connected graph,'' Discrete Math. 293 (2005), no. 1-3, 61--72.

[51] Ando, Kiyoshi; Kane ko, Atsushi; Kawara bayashi, Ken-ichi,``Vertices of degree 5 in a contraction critically 5-connected graph,'' Graphs Combin. 21 (2005), no. 1, 27--37.

[52] I G. B. Baskara Nugraha, M. Nishiara, and H. Morita, ``A Hybrid Multicast Communication System for Internet Video Broadcasting,'' Transactions on Electrical Eng., Electronics, and Communications, vol. 4, no. 2, pp. 103-111, 2006.

[53] I G. B. Baskara Nugraha, S. Marugami, M. Nishiara, H. Morita, ``Multicast Communication for Video Broadcasting Service over IPv4 Network Using IP Option,'' IEICE Trans. Communications, vol. E98-B, no. 5, pp. 1570-1580, 2006.

[54] Yasuhiro Takahashi and Noboru Kunihiro, ``A quantum circuit for Shor's factoring algorithm using 2n+2 qubits,'' Quantum Information and Computation, Vol.6 No.2, pp.184-192, 2006.

[55] Yuichi Komano and Kazuo Ohta, ``Taxonomical Security Consideration of OAEP Variants,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp. 1233-1245, 2006.

[56] Mitsugu Iwamoto, Lei Wang, Kazuki Yoneyama, Noboru Kunihiro and Kazuo Ohta, ``Visual Secret Sharing Schemes for Multiple Secret Images Allowing the Rotation of Shares,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp.1382-1395 , 2006.

[57] N. Kunihiro W. Abe and K. Ohta, ``Maurer-Yacobi ID based Key Distribution Revisited,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp. 1421-1424, 2006.

[58] 伊豆哲也, 國廣昇, 太田和夫, 武仲正彦, ``双線形写像を用いた墨塗り署名方式の安全性について, '' 情報処理学会論文誌, Vol. 47, No. 7, pp.2409-2416, 2006.

[59] Hyun-Ho Kang, Brian Kurkoski, Young-Ran Park, Hye-Joo Lee, Sang-Uk Shin, Kazuhiko Yamaguchi, Kingo Kobayashi, ``A Viable System for Tracing Illegal Users of Video,'' Lecture Notes in Computer Science, Vol. 3917 (International Workshop, WISI 2006), pp. 156-158, Springer-Verlag, 2006.

[60] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, ``Tracing Illegal Users of Video : Reconsideration of Tree-Specific and Endbuyer-Specific Methods・ Accepted for publication in Lecture Notes in Computer Science, (4th Workshop on Internet Communications Security, WICS2006), Springer-Verlag,2006.

[61] Masazumi Kurihara, ``Decoding algorithm for Iterated codes correcting compund- errors,'' Electronics and Communications in Japan, Part 3, Vol.3. No.1, pp.60-72, 2006.

[62] Tien Duc Nguyen, Xuan Nam Tran, and Tadashi Fujino, ``Layer error?characteristics of lattice-reduction aided V-BLAST detectors,'' IEICETran. Fundamentals, Vol. E89-A, No. 10, pp.2535-2542, Oct. 2006.

[63] M. Iwamoto, L. Wang, K. Yoneyama, N. Kunihiro, and K. Ohta, ``Visual Secret Sharing Schemes for Multiple Secret Images Allowing the Rotation of Shares,'' IEICE Trans. on Fundamentals, vol.E89.A, no.5, pp.1382-1395, May, 2006.

[64] M.Iwamoto and H.Yamamoto, ``Strongly Secure Ramp Secret Sharing Schemes for General Access Structures,'' Information Processing Letters, Vol 97, Issue 2, pp.52-57, 2006.

[65] Komuro, Hideo; Ando, Kiyoshi; Nakamoto, Atsuhiro, ``Tight quadrangulations on the sphere, ''

Discrete Math. 306 (2006), 61--72.

[66] H. Nagaoka and M. Hayashi, ``An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses,'' IEEE Trans. on Inform. Theory, vol.53, no.2, pp.534-549, 2007.

[67] 西新 幹彦, 渡邊 大, 森田 啓義, ``算術符号における符号語の生成過程の確率モデルについて,''
電子情報通信学会論文誌 A, vol. J90-A, no. 2, pp. 170-174, 2007.

[68] M. Iwamoto, H. Yamamoto, and H. Ogawa, ``Optimal Multiple Assignments Based on Integer Programming in Secret Sharing Schemes with General Access Structures,'' IEICE Trans. on Fundamentals, vol.E90.A, no.1, pp. 101-112, Jan., 2007.

[69] Yu SASAKI, Yusuke NAITO, Noboru KUNIHIRO and Kazuo OHTA, ``Improved Collision Attacks on MD4 and MD5,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp. 36-47, 2007.

[70] Yuichi KOMANO, Kazuo OHTA, Atsushi SHIMBO and Shinichi KAWAMURA, ``Toward the Fair Anonymous Signatures: Deniable Ring Signatures,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp. 54-64, 2007.

[71] Haruki OTA, Kazuki YONEYAMA, Shinsaku KIYOMOTO, Toshiaki TANAKA and Kazuo OHTA,``Universally Composable Hierarchical Hybrid Authenticated Key Exchange,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.1, pp. 139-151, 2007.

[72] Yasuhiro Takahashi, Noboru Kunihiro, and Kazuo Ohta,``The Quantum Fourier Transform on a Linear Nearest Neighbor Architecture,'' Quantum Information and Computation, Vol.7 No.4, pp.383-391, 2007.

[73] Yoshikazu Hanatani, Yuichi Komano, Kazuo Ohta and Noboru Kunihiro, ``Provably Secure Untraceable Electronic Cash against Insider Attacks,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No.5, 2007, to appear.

[74] Ando, Kiyoshi, ``Contractible Edges in a k-Connected Graph,'' Discrete Geometry, Combinatorics and Graph Theory, LNCS 4381, (2007), 10--21. endthebibliographyI

招待講演発表

[1] 韓太舜, ``情報スペクトルから見た情報理論(IEICE Fellow 受賞講演),'' 基礎・境界ソサエティ全国大会, 電子情報通信学会, 東北大学, 2003.

[2] Te Sun Han,``A Forlore in Information Theory,'' Fundamental Concepts in Information Theory(Invited lecture), '' Kamogawa, Japan, June 25-28; Proc. 3rd Asian-European Workshop on Information Theory, pp.61-63, 2003.

[3] Te Sun Han,``A Forlore in Sorce coding : Information-spectrum approach,'' シャノン理論ワークショップ STW03, 第1回シャノン理論ワークショップ(STW03)予稿集, pp.1-6, 2003.

[4] 韓太舜, ``情報スペクトル:あれこれ,'' Information-Spectrum Approaches: Tutorial, 電子情報通信学会・情報理論研究会, 電子情報通信学会技術研究報告, IT2003-54, 2003. vol.103, No.498, pp.31-39, 2003

[5] 小林欣吾, ``情報理論の愉しみ(IEICE Fellow 受賞講演),'' 基礎・境界ソサエティ全国大会, 電子情報通信学会, 電気通信大学, 2004.

[6] H. Nagaoka,``Differential Geometrical Aspects of Quantum Estimation Theory'', COE-Kakenhi workshop on Quantum Information Theory and Quantum Statistical Inference, Proc. pp.9-11, Tokyo, 2005.

[7] H. Nagaoka,``A Quantum/Complex Extension of Information Geometry'', The 2nd International Symposium on Information Geometry and Its Applications, Proc. pp.177-180, Tokyo, 2005.

[8] Kiyoshi Ando, ``Contractible edges in k-connected graphs,'' The China-Japan Joint Conference on Discrete Geometry, Combinatorics and Graph Theory, Nankai University (Tianjin, China) and Northwestern Polytechnical University (Xi'an, China), Nov. 18-24, 2005.

[9] T. Kawabata, ``Text Compression Algorithms --An Approach from Probabilistic Modelling--,''
Tutorial workshop on game-theoretic probability and related topics, Mar. 2006.

[10] 川端 勉, ```無歪みデータ圧縮入門--算術符号とCTW法を中心として,''情報とダイナミックス研究集会, Aug. 2006.

[11] 岩本貢, ``''秘密分散法に対する符号化定理,'' 電子情報通信学会 ソサイエティ大会 チュートリア
ル講演, AT-1-4, Sept., 2006.

[12] Tadashi Fujino, ``Multi-Carrier CDMA System for Combating Channel Blocking in Frequency-Selective Fading MIMO Channel,'' The 10th Biennial Radio Electronics Conference on Radio & Electronics (REV'06), Hanoi, Vietnam, Nov. 2006.

[13] S. Sakata, ``On the Berlekamp-Massey-Sakata algorithm,'' Workshop on Gr ''obner Bases in Cryptography, Coding Theory and Algebraic Combinatorics, April 30 -- May 6, Semester on Gr ''obner Bases And Related Methods 2006, Linz, Austria, 2006.

[14] S. Sakata, ``Applications of the BMS algorithm to decoding of codes from curves,'' Workshop on Gr ″obner Bases in Cryptography, Coding Theory and Algebraic Combinatorics, April 30 -- May 6, Semester on Gr ″obner Bases And Related Methods 2006, Linz, Austria, 2006.

[15] 阪田省二郎, ``符号・配列・グレブナー基底, グレ ブナー基底,'' 夏の学校, 京都大学数理解析研究所, August 28 -- September 1, 2006.

[16] 阪田省二郎, ``代数的符号理論:夢と現実,'' 電子情報通信学会技術報告, IT2006-49, pp.25--32: 電子情報通信学会情報理論研究会, 若手研究者のための講演会, 函館, 北海道, November 28, 2006

[17] H. Nagaoka, ``On quantum extension of information geometry,'' International Workshop on Affine Differential Geometry and Information Geometry, 成都, 中国, 2006.

[18] H. Nagaoka, ``On the error exponents of quantum hypothesis testing,'' Special seminar series on quantum information, National Institute of Informatics, 2007.

[19] 長岡浩司, ``統計力学と量子情報の数理,'' シンポジウム「量子系におけるコトの物理学」, 日本物理学会 2007 年春季大会, 2007(発表予定).

国際学会プロシーディングス(査読あり)

[1] S. Sakata, ``Synthesis of the simplest linear feedback shift register allowing prescribed pairs
of input and output sequences --- A fast algorithm for solving discrete-time Wiener-Hopf equations,'' it Proc. of IEEE Intern. Symp. Inform. Theory (ISIT-2002), p.58, Lausanne, Switzerland, June 30--July 5, 2002.

[2] Shojiro Sakata, ``Efficient factorization methods for list decoding of code from curves,'' Proc. of 2003 IEEE Intern. Symp. Inform. Theory, 363, Yokohama, Japan, June 29--July 4, 2003.

[3] T.Fujino, ``An Anti-Blocking Multicarrier CDMA System in MISO Channel with Time Diversity'',
IEEE Symposium on Signal Processing and Information Technology, Rome, Italy, 2004.

[4] X.N.Tran, T.Fujino and Y.Karasawa, ``On performance of multiuser OFDM systems with transmit diversity,'' IEEE Symposium on Signal Processing and Information Technology, Rome, Italy, 2004.

[5] X.N.Tran, T.Fujino and Y.Karasawa, ``An MMSE detector for multiuser space-time block coded OFDM,'' 9th Int. OFDM Workshop, Dresden, Germany, September, 2004.

[6] T.Fujino, ``An Anti-Blocking Multicarrier CDMA System in the MISO Channel'', 9th Int. OFDM Workshop, Dresden, Germany, September, 2004.

[7] X.N.Tran, A.Rajapakshe, T.Fujino, and Y.Karasawa, ``Performance of space-time block coded CDMA systems with adaptive beamforming,'' 2004 Int. Symp. Antenna and Propagation, Sendai, Japan, Aug. 2004.

[8] Shojiro Sakata, , ``Multiple-Sequence BM Algorithm can be Replaced by a Succession of Single-Sequence BM Algorithm,'' Proc. 2005 IEEE International Symposium on Information Theory, pp. 1967-1971, Adelaide, Australia, 2005.

[9] Masaya Fujisawa, Shojiro Sakata, , ``A Class of Quasi-Cyclic Regular LDPC Codes from Cyclic Difference Families with Girth 8,'' Proc. 2005 IEEE International Symposium on Information Theory, pp. 2290-2294, Adelaide, Australia, 2005

[10] Kansuke Onishi, Mamoru Hoshi, ``Optimal region for binary search tree, rotation and polytope,'' Proc. of the 5th International Symposium on Operations Research and Its Applications, Lhasa, Tibet, China, 255 - 266, August 8-13, 2005.

[11] Motohiro Nakanishi, Michihiro Kobayakawa, Mamoru Hoshi, Tadashi Ohmori, ``A Method for Extracting a Musical Unit to Phrase Music Data in the Compressed Domain of TwinVQ Audio Compression,'' Proc. of Int. Conf. on Multimedia and Expo (ICME2005), 2005.

[12] M. M. Rashid, T. Kawabata, ``Theoretical Analysis of a Zero-redundancy Estimator with a Finite Window for Memoryless Source,'' IEEE ITSOC Information Theory Workshop on Coding and Complexity, pp.171-175, 2005.

[13] Tsutomu Kawabata and You Yanagisawa, ``Redundancy of Symbol Decomposition Algorithms for Memoryless Source,'' Proceedings of 2005 IEEE International Symposium on Information Theory, pp.500-504, 2005.

[14] Jun-ichi Takeuchi, Andrew Barron, Tsutomu Kawabata, ``Statistical Curvature and Stochastic Complexity, '' Proceedings of the Second International Symposium on Information Geometry and its Applications, 2nd IGAIA, pp.29-36, 2005.

[15] N. Yapage and H. Nagaoka, ``A Quantum Extension of Boltzmann Machine: An Information Geometrical Approach'', Proc. of Erato conference on Quantum Information Science (EQIS) 2005, pp.204-205, Tokyo (2005).

[16] M. Arimura and H. Nagaoka, ``An Extension of Asymptotically Sufficient Statistic Method for Pointwise Strong Universality,'' Proc. 2005 IEEEInternational Symposium on Information Theory, pp. 505-509, Adelaide, Australia, 2005.
H. Morita, M. Satoh, and A. J. van Wijngaarden, ``On Multimode Polarity-Switch Codes of Rate 1-1/n,'' Proc. 2005 IEEE International Symposium on Information Theory, pp. 387-391, Adelaide, Australia, 2005.

[17] Hiroyoshi Morita and Takahiro Ota, ``A Tight Upper Bound on the Size of the Antidictionary of a Binary String,'' Proceedings of Analysis of Algorithms 2005, Barcelona, Spain, June 2005.
Ken-ichi Iwata, ``On Multiple-Access Communication System for General Correlated Sources with an Array of General Independent Channels,'' Proc. 2005 IEEE International Symposium on Information Theory, pp. 142-146, Adelaide, Australia, 2005.

[18] I Gusti Bagus Baskara Nugraha, Mikihiko Nishiara, Hiroyoshi Morita, ``A Hybrid Multicast Communication System for Internet Video Broadcasting,'' International Symposium on Communications and Information Technologies, pp.190-193, 2005.
T.Fujino and J.Nakamura, ``A Multicarrier CDMA System for Combating Channel Blocking in Frequency-Selective Fading MIMO Channel '', IEEE Symposium on Signal Processing and Information Technology, Athens, Greece, Dec. 2005.

[19] X.N. Tran, and T.Fujino, ``Groupwise succeessive ICI cancellation for OFDM systems in time-varying channels,'' IEEE Symposium on Signal Processing and Information Technology, Athens, Greece, Dec. 2005.

[20] T.Fujino and J.Nakamura, ``A proposal of Multicarrier CDMA system for combating channel blocking in frequency-selective Rayleigh fading MIMO channel'', IEE Int. Conf. on 3G &Beyond, London, UK, Nov. 2005.

[21] A.T.Le, X.N. Tran, and T.Fujino,``Combined MMSE-ML multicarrier detection with reduced complexity forSTBC-OFDM systems,″ IEE Int. Conf. on 3G &Beyond, London, UK, Nov. 2005.
Y. Naito, Y. Sasaki, N. Kunihiro and K. Ohta, ``Improved Collision Attack on MD4 with Probability Almost 1,″ ICISC2005, 2005.

[22] Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, ``On the Security of Probabilistic Multisignature Schemes and their Optimality,″ MyCrypt2005, pp.132-150, 2005.

[23] Y. Takahashi and N. Kunihiro, ``A linear-size quantum circuit for addition with no ancillary qubits,″ EQIS2005, pp.113-114, 2005.

[24] N. Kanayama, M. Kida, N. Kunihiro, T. Nishino, K. Ohta and S. Okubo, ``Quantum Algorithms for Solving Exact Shortest Vector Problem,″ EQIS2005, pp.179-180, 2005.

[25] T. Izu and N. Kunihiro, K. Ohta and T. Shimoyama, ``Analysis on the Clockwise Transposition Routing for Dedicated Factoring Devices,″ WISA2005, pp. 232-242, 2005.

[26] Hyun-Ho Kang, Brian Kurkoski, Young-Ran Park, Hye-Joo Lee, Sang-Uk Shin, Kazuhiko Yamaguchi, Kingo Kobayashi, ``Video Fingerprinting System using Wavelets and Error Correcting Codes,″ in Proceedings of 6th International Workshop on Information Security Applications 2005 (WISA 2005), pp. 323-338.

[27] Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, ``On BCJR State Metric Quantization for Turbo Equalization,″ in Proceedings of the International Symposium on Information Theory, pp. 234-238, Sept. 2005.

[28] Brian Kurkoski, Paul Siegel, Jack Wolf, ``Soft-output Detector for Partial-Response Channels Using Vector Quantization,″ in Digests of the IEEE International Magnetics Conference, p. 801, April 2005.

[29] Kamal Elkhaili, Tsutomu Kawabata, ``Broadcasting for Dirty Printers,″ Proceedings of 2006 IEEE International Symposium on Information Theory,Seattle, Sep. 2006.

[30] M. Mambo, M. R. Salinas, K. Ohta and N. Kunihiro, ``Problems on the MR Micropayment Schemes,″ in Proceedings of ASIACCS2006.

[31] Yuichiro Esaki, Noboru Kunihiro and Kazuo Ohta, ``Untraceable Off-Line Verifiable Quantum Cash,″ in Proc. of TQC2006.

[32] Y. Hanatani, Yuichi Komano, Kazuo Ohta and Noboru Kunihiro, `Provably Secure Electronic Cash based on Blind Multisignature Schemes, " 10th Financial Cryptography and Data Security Conference (FC 06).

[33] Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, ``Toward the Fair Anonymous Signatures: Deniable Ring Signature," CT-RSA2006, pp. 174-191, 2006.

[34] T.D.Nguyen, X.Nam Tran, and T.Fujino, ``Layer error characteristics of lattice-reduction aided V-VLAST detectors," IEEE Symposium on Personal, Indoor, Mobile, and Radio Communications (PIMRC), Helsinki, Finland, Sept. 2006.

[35] X.N.Tran, Cong Huan Ho, and T.Fujino, ``On performance of dtetection methods for combined STBC and SM systems," The 10th Biennial Radio Electron. Conf. on Radio & Electron. (REV'06), Hanoi, Vietnam, Nov.2006.

[36] T.D.Nguyen, X.N.Tran and T.Fujino, ``On suboptimality of lattice-reduction aided V-BLAST detectors" The 10th Biennial Radio Electron. Conf. on Radio & Electron. (REV'06), Hanoi, Vietnam, Nov. 2006.

[37] Van Duc Nguyen, X.N.Tran, and T.Fujino, ``Dynamic sub-carrier allocation for multiuser OFDMA/TDD networks with full f requency reuse", The 10th Biennial Radio Electron. Conf. on Radio & Electron.(REV'06), Hanoi, Vietnam, Nov. 2006.

[38] Brian Kurkoski, Kazuhiko Yamaguchi, ``Turbo Equalization as a Post-Processor for Partial-Response Channels," to appear in Digests of the 2006 IEEE International Magnetics Conference.

[39] N. Yapage and H. Nagaoka, ``Information geometry of mean field approximation for quantum Boltzmann machines," Asian Conference on Quantum Information Science (AQIS) 2006, pp.143-144 in Proceedings, 北京, 中国, 2006.

査読なし国際会議, 国内発表

[1] 藤沢匡哉, 木村崇, 阪田省二郎, ``巡回差集合に基づく準巡回 LDPC 符号について,"電子情報通信学会技術報告, IT2004-41, pp.19--24, 2004.

[2] S. Sakata, ``Parallel BM algorithm and Euclidean algorithm for decoding are identical," (Eds. U. Mengali, H. Yamamoto) Proceedings of 2004 International Symposium

on Information Theory and its Applications (ISITA-2004), Parma, Italy, October 10 -- 13, 2004.

[3] 岩本貢, 山本博資, ``強い秘密保護特性をもつランプ型秘密分散法,'' 情報理論とその応用シンポジウム(SITA) 2004, pp.331-334, Dec., 2004.

[4] S. Sakata, ``Some more remarks on 1D / mD linear recurrences and their applications,'' Workshop on Coding Theory, Lyngby, Denmark, June 2 -- 3, 2005.

[5] S. Sakata, ``Recent developments of coding theory related to Grobner basis,'' Workshop on Theoretical Effectivity and Practical Effectivity of Grobner Bases, 立教大学,東京, August 22 -- 26, 2005.

[6] 大西 建輔,小早川 倫広,木村 彰宏,星 守,大森 匡, ``任意のLp距離関数による検索が可能な索引構造,'' 情報処理学会研究会報告 アルゴリズム研究会, AL-103, pp. 67--76,2005.
正津宗幸,栗原正純,杉村立夫, ``Reed-Solomon 符号の最尤復号に関する検討,'' IEICE Tech. Report, IT2005-54, Vol.105, No.311, pp.19-24, 2005.

[7] Kamal Elkhaili, Tsutomu Kawabata, ``Broadcasting for Dirty Printers,'' Proceedings of the 28th Symposium on Information Theory and Its Applications, Vol. 1, pp. 67-70, 2005.

[8] 太田隆博,森田啓義, ``Suffix tree を用いた反辞書の生成法について,'' 信学技報, July 2005.

[9] Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, ``Turbo Decoding Based on the Lookup-Table Algorithm,'' 第 28 回情報理論とその応用シンポジウム予稿集(Proceedings of the 28th Symposium on Information Theory and its Applications), pp. 503-506, 2005.

[10] 前原進也,ブライアン クルカスキー,山口和彦,小林欣吾, ``Reed-Solomon 符号の硬判定復号を用いた連接符号のターボ復号の評価,'' 第 28 回情報理論とその応用シンポジウム予稿集 (Proceedings of the 28th Symposium on Information Theory and its Applications), pp. 351-354, 2005.

[11] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, ``Tracing Illegal Users of Video Content Using Watermarking and Fingerprinting,'' 第 28 回情報理論とその応用シンポジウム予稿集 (Proceedings of the 28th Symposium on Information Theory and its Applications), pp. 483-486, 2005.

[12] Brian Kurkoski, Kazuhiko Yamaguchi, ``Vector Quantization of Convolutional Decoder State Metrics,'' in Proceedings of Hawaii, IEICE and SITA Joint Conference on Information Theory, 電子情報通信学会技術 報告情報理論, IT2005-21, pp. 15-20, 2005.

[13] Masato Yabe, Kazuhiko Yamaguchi, Brian Kurkoski, Kingo Kobayashi, ``A Decoding Algorithm for LDPC Codes using Threshold Control for the Burst Error Channel,'' in Proceedings of Hawaii, IEICE and SITA Joint Conference on Information Theory, 電子情報通信学会技術報告情報理論, IT2005-21, pp. 121-124, 2005.

[14] S. Sakata, M. Fujisawa,`` An extension of BMS algorithm and decoding of two-point AG codes,''第 28 回情報理論とその応用シンポジウム予稿集, pp.539--542, 恩納村, 沖縄, November 20--23, 2005.

[15] 藤沢匡哉, 阪田省二郎, ``1点代数曲線符号に対する Sudan 法に基づいた高速限界距離復号法について,''第 28 回情報理論とその応用シンポジウム予稿集, pp.543--546, 恩納村, 沖縄, November 20--23, 2005.

[16] Takahiro Ota and Hiroyoshi Morita, ``Linear Complexity Construction of Antidicitonaries,'' Proc. of the 28th Symposium on Information Theory and its Applications (SITA2005), Onna, Okinawa, pp.407--410, Nov. 2005.

[17] 山本 敦,小早川 倫広,星 守,大森 匡, ``画像の領域分割に基づく類似画像検索,'' 情報処理学会研究会報告オーディオビジュアル複合研究会, AVM-52, pp.19--26, 2006.
太田隆博,森田啓義, ``反辞書木情報源モデルを用いたデータ圧縮,'' 信学技報, 名古屋, Mar. 2006.

[18] 渡邊大,西新幹彦,森田啓義, ``算術符号における符号語の生成過程の確率モデルについて'', 信学技報, 名古屋, Mar. 2006.

[19] 島貫至行,ブライアン クルカスキー,山口和彦, ``Turbo-like 符号による低符号化率連接号の 二、三の考察,'' 電子情報通信学会技術報告情報理論, 2006 年 3 月掲載予定.

[20] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, ``Tracing Illegal Users of Video Content: Reconsideration of Tree-Specific and Endbuyer Specific Methods,''電子情報通信学会 2006 年 暗号と情報セキュリティシンポジウム, 2006.

[21] 栗原正純,楯岡孝道, ``組合せネットワーク上のルーティング制御とその応用,'' IEICE Tech. Report, Vol.105 No.662, IT2005-131, pp.211-216, 2006.

[22] Neji Youssef, Tsutomu Kawabata, ``On the distribution densities of capacity fade and inter-fade
time intervals over SISO Rayleigh mobile fading channels,''IEICE Technical Report, AP2006-81,pp.39-34, Oct. 2006.

[23] 竹内 純一, 川端 勉, ``木情報源と確率的コンプレクシティ,'' シャノン理論ワークショップ、情報理論とその応用学会、Sep. 2006.

[24] 川端 勉, 竹内 純一,``離散定常情報源の確率構造について,''第29回情報理論とその応用シンポジウム予稿集, pp.161-164,Nov.,2006

[25] 小野 博督, 川端 勉, ``二次元ガウス密度に対する二段階一様格子量子化器の設計,''第29回情報理論とその応用シンポジウム予稿集, pp.887-890, Nov.,2006.

[26] 小林 且弥, 川端 勉, ``マルコフ情報源に対する文脈依存増分分解法の性能評価について,''第29回情報理論とその応用シンポジウム予稿集, pp.883-886,Nov.,2006.

[27] S. Sakata, M. Fujisawa, ``a comparison between WB algorithm and BM algorithm,'' (Eds. H. Chung, T. Fujiwara) CD-ROM: Proceedings of 2006 International Symposium on Information Theory and its Applications (ISITA-2006), Seoul. Korea, October 10 -- 13, 2006.

[28] S. Sakata, M. Fujisawa, ``WB-like decoding algorithm of one-point codes from curves,''第29 回情報理論とその応用シンポジウム予稿集, pp.93--96, 函館, 北海道, November 28 -- December 1, 2006.

[29] M. Fujisawa, H. Matsui, M. Kurihara, S. Sakata, ``With a higher probability one can correct errors up to half the designed distance for primal codes from curves,''第 29 回情報理論とその応用シンポジウム予稿集, pp.101--104, 函館, 北海道, November 28 -- December 1, 2006.

endthebibliographyI など多数

著書, 解説記事

[1] Fred Piper, Sean Murphy (著), 太田 和夫, 國廣 昇 (翻訳),暗号理論, 岩波書店, 2004 年 3 月.

阪田省二郎, ``代数的符号理論,'' 「数理科学」2004 年 11 月号, 特集: 符号化理論の新時代, pp.19--29.

[2] 太田 和夫, ``公開鍵暗号の安全性評価,'' 情報セキュリティハンドブック第 2 編 11 章, 電子情報通信学会編, オーム社, 2004 年 11 月.國廣昇, 太田 和夫, ``暗号の米政府標準方式が危機に,''「科学」解説, 岩波書店, 2005 年 11 月号 pp.1235-1237.

[3] H. Nagaoka, Asymptotic Theory of Quantum Statistical Inference, (ed. M. Hayashi), World Scientific (2005).

[4] 太田和夫,國廣昇,「ほんとうに安全？現代の暗号」,岩波書店,2005 年 5 月.

[5] 阪田省二郎,栗原正純,松井一,藤沢匡哉,「誤り訂正符号入門」,森北出版株式会社, 2005.

[6] 國廣昇,太田和夫,「暗号の米政府標準方式が危機に」,岩波書店「科学, 2005 年 11 月号, p.1235-1237.

[7] 阪田省二郎、栗原正純、松井一、藤沢匡哉 (共訳)、誤り訂正符号入門、森北出版、2005 (原著: J. Justesen,T. Hoeholdt, A Course in Error-Correcting Codes, EuropeanMathematical Society, 2004).

[8] 阪田省二郎, 符号・配列・グレブナー基底, 日比孝之(編)「グレブナー基底の現在」 第 6 章, pp.128--152, 数学書房, 2006.