研究業績リスト

2021年1月25日現在

著書等

B1）単行本，「現代数理科学事典 第二版」，部門8 情報の理論，ワーキングメンバ，および，量子誤り訂正符号の解説，丸善出版株式会社，2009/12 発刊.

B2）単行本「符号理論 ～デジタルコミュニケーションのための数学～」，萩原学，日本評論社，2012/8/10 発刊.

B3）単行本「進化する符号理論」，編著+一部執筆 萩原学，日本評論社，2016/9/9 発刊.

B4）単行本「Coq/SSReflect/MathComp による定理証明:フリーソフトではじめる数学の形式化」，萩原学，アフェルト・レナルド，森北出版，2018/4 発刊.

受賞 本人(共著含む)

A1) Outstanding Paper Award (in the ICACT2014 International Conference hosted by the Global IT Research Institute with IEEE Communication Society), Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura, 2014/2/17.

A2) I-Scover プロジェクト功績賞, 萩原学, 電子情報通信学会, 2017/3.

A3) 電子情報通信学会 功績賞(ソサイエティ運営), 萩原学, 電子情報通信学会, 2019/9.

A4) 電子情報通信学会 功績賞(サブソサイエティ運営), 萩原学, 電子情報通信学会, 2020/9.

受賞 指導学生

AS1) Justin Kong, Binary Multipermutation Ulam Sphere Analysis, 2017 年 SITA 若手研究者論文賞受賞者.

AS2) 中山歩, 単一削除誤りに対する量子誤り訂正符号の構成, 情報理論研究会(2020 年 1 月 24 日), 情報理論とその応用サブソサイエティ学生優秀発表賞, 2019 年度後期.

査読有り論文誌（含 Springer Lecture Note）

J1) Minuscule Heaps over Dynkin Diagrams of Type ¥tilde A, Manabu Hagiwara, The Electronic Journal of Combinatorics, vol. 11 (2004), R3, 20pp, -no publisher-, 2004/01.
DOI: https://doi.org/10.37236/1756

J2) A characterization of the simply-laced FC-finite Coxeter groups, Manabu HAGIWARA, Masao ISHIKAWA, Hiroyuki TAGAWA, Annals of Combinatorics, Springer, pp.177-196, 2004/08.
DOI: https://doi.org/10.1007/s00026-004-0214-6

J3) 2h(2j+1)準位量子状態に対する非スタビライザ型クリフォード符号構成, 萩原 学, 今井 秀樹, 電子情報通信学会論文誌 A 基礎・境界, J88-A-8, pp.917-921, 2005/08.

J4) A Construction for Non-Stabilizer Clifford Code, Manabu HAGIWARA, Hideki IMAI, REALIZING CONTROLLABLE QUANTUM STATES, pp.304-309, World Scientific, 2005/11.

J5) A Short Random Fingerprinting Code against a Small Number of Pirates, Manabu HAGIWARA, Goichiro Hanaoka, Hideki Imai, LECTURE NOTES IN COMPUTER SCIENCE, 3857, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings, pp.193-202, Springer, 2006/02.
DOI: https://doi.org/10.1142/9789812701619_0047

J6) Unconditionally Secure Chaffing-and-Winnowing: A Relationship between Encryption and Authentication, Goichiro Hanaoka, Yumiko Hanaoka, Manabu HAGIWARA, Hajime Watanabe, Hideki Imai, LECTURE NOTES IN COMPUTER SCIENCE, 3857, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings, pp.154-162, Springer, 2006/02.
DOI: https://doi.org/10.1007/11617983_15

J7) On the Key-Privacy Issue of McEliece Public-Key Encryption, Shigeki Yamakawa, Cui Yang, Kazukuni Kobara, Manabu HAGIWARA, Hideki Imai, LECTURE NOTES IN COMPUTER SCIENCE, 4851, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Proceedings, pp.168-177, Springer, 2007/12.
DOI: https://doi.org/10.1007/978-3-540-77224-8_21

J8) An Improvement of Tardos's Collusion-Secure Fingerprinting Codes with Very Short Lengths, Koji Nuida, Satoshi Fujitsu, Manabu HAGIWARA, Takashi Kitagawa, Hajime Watanabe, Kazuto Ogawa, Hideki Imai, LECTURE NOTES

IN COMPUTER SCIENCE, 4851, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Proceedings, pp.80-89, Springer, 2007/12.
DOI: https://doi.org/10.1007/978-3-540-77224-8_12

J9) Optimization of Tardos's Fingerprinting Codes in a Viewpoint of Memory Amount, Koji Nuida, Manabu HAGIWARA, Hajime Watanabe, Hideki Imai, Information Hiding, LECTURE NOTES IN COMPUTER SCIENCE, 4567, Information Hiding, Revised Selected Papers, pp.279-293, Springer, 2008/01.
DOI: https://doi.org/10.1007/978-3-540-77370-2_19

J10) Error-correcting codes and cryptography, Hideki Imai, Manabu HAGIWARA, APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING, 19-3, pp.213-228, Springer, 2008/04.
DOI: https://doi.org/10.1007/s00200-008-0074-0

J11) An Efficient 2-Secure and Short Random Fingerprint Code and its Security Evaluation, Koji Nuida, Satoshi Fujitsu, Manabu HAGIWARA, Hideki Imai, Takashi Kitagawa, Kazuto Ogawa, Hajime Watanabe, IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES, 92-1, pp.197-206, IEICE, 2009/01.
DOI: https://doi.org/10.1587/transfun.E92.A.197

J12) An improvement of discrete Tardos fingerprinting codes, Koji Nuida, Satoshi Fujitsu, Manabu HAGIWARA, Takashi Kitagawa, Hajime Watanabe, Kazuto Ogawa, Hideki Imai, DESIGNS CODES AND CRYPTOGRAPHY, Vol.52, 3, pp.339-362, Springer, 2009/04.
DOI: https://doi.org/10/1007/s10623-009-9285

J13) Bounds on the Number of Users for Random 2-Secure Codes, Manabu HAGIWARA, Takahiro Yoshida, Hideki Imai, LECTURE NOTES IN COMPUTER SCIENCE, 5527, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Proceedings, pp.239-242, Springer, 2009/06.
DOI: https://doi.org/10.1007/978-3-642-02181-7_29

J14) Smallest Size of Circulant Matrix for Regular Quasi-Cyclic LDPC Codes with Girth at Least 6, Manabu HAGIWARA, Takashi Kitagawa, Marc Fossorier, Hideki Imai, IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, E92-A-11, pp.2891-2894, IEICE, 2009/11.
DOI: https://doi.org/10.1587/transfun.E92.A.2891

J15) Quantum Error Correction Beyond the Bounded Distance Decoding Limit,

Kenta Kasai, Manabu HAGIWARA, Hideki Imai, Koichi Sakaniwa, IEEE TRANSACTIONS ON INFORMATION THEORY, 58-2, pp.1223-1230, 2012/02.
DOI: https://doi.org/10.1109/TIT.2011.2167593

J16) Fixed Initialization Decoding of LDPC codes over a Binary Symmetric Channel, Manabu HAGIWARA, Marc Fossorier, Hideki Imai, IEEE TRANSACTIONS ON INFORMATION THEORY, 58-4, pp.2321-2329, 2012/04.
DOI: https://doi.org/10.1109/TIT.2011.2177440

J17) LP Decodable Permutation Codes based on Linearly Constrained Permutation Matrices, Tadashi Wadayama, Manabu Hagiwara, IEEE TRANSACTIONS ON INFORMATION THEORY, 58-8, pp.5454-5470, IEEE, 2012/8.
DOI: https://doi.org/10.1109/TIT.2012.2196253

J18) A Numerical Evaluation of Entanglement Sharing Protocols Using Quantum LDPC CSS Codes, Masakazu Yoshida, Manabu Hagiwara, Takayuki Miyadera, Hideki Imai, IEICE TRANSACTION on Fundamentals of Electronics, Communications and Computer Sciences Vol.E95-A No.9, pp.1561-1569, IEICE, 2012/09.
DOI: https://doi.org/10.1587/transfun.E95.A.1561

J19) 同期誤りと反転誤り訂正に適した LDPC 符号とスライド復号法，重廣亨，矢部裕久，岩村恵市，萩原学，電子情報通信学会論文誌 B，Vol.J96-B，No.10，pp.1230-1237，2013.

J20) Formalization of Shannon's Theorems, Reynald Affeldt, Manabu Hagiwara, and Jonas Sénizergues, Journal of Automated Reasoning, 53(1), pp.63-103, Springer, 2014. DOI: https://doi.org/10.1007/s10817-013-9298-1

J21) Performance Analysis for PUF Data Using Fuzzy Extractor, Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura, Lecture Note in Electrical Engineering, Vol. 280, Ubiquitous Information Technologies and Applications, Proceedings, pp.277-284, Springer, 2014.
DOI: https://doi.org/10.1007/978-3-642-41671-2-36

J22) A short proof for the multi-deletion error correction property of Helberg codes, Manabu Hagiwara, IEICE Communications Express, Vol.5 (2016) No.2, pp.49-51, IEICE, 2016.
DOI: https://doi.org/10.1587/comex.2015XBL0182

J23) Consolidation for compact constraints and Kendall tau LP decodable permutation codes, Manabu Hagiwara, Justin Kong, Designs, Codes and Cryptography, vol.85, issue 3, pp.483-521, Springer, 2017/12.

DOI: https://doi.org/10.1007/s10623-016-0313-5.

J24) Formalization of Bing's Shrinking Method in Geometric Topology, Ken'ichi Kuga, Manabu Hagiwara and Mitsuharu Yamamoto, Lecture Notes in Artificial Intelligence, 9791, Intelligent Computer Mathematics, Proceedings, pp.18-27, Springer, 2016.
DOI: https://doi.org/10.1007/978-3-319-42547-4_2

J25) The first Quantum Error-Correcting Codes for Single Deletion Errors, Ayumu Nakayama, Manabu Hagiwara, IEICE Communications Express, Vol.9, Issue 4, pp.100-104, IEICE, 2020.
DOI: https://doi.org/10.1587/comex.2019XBL0154

J26) A Number Theoretic Formula and Asymptotic Optimality of Cardinalities of BAD Correcting Codes, Takehiko Mori, Manabu Hagiwara, Discrete Mathematics, 343 (6), Elsevier, 2020/06.
DOI: https://doi.org/10.1016/j.disc.2020.111852

J27) Applications of Gaussian binomials to Coding Theory for Deletion Error Correction, Manabu Hagiwara, Justin Kong, Annals of Combinatorics, vol.24, pp.379-393, 2020/06.
DOI: https://doi.org/10.1007/s00026-020-00494-4

J28) Perfect Multi Deletion Codes Achieve the Asymptotic Optimality of Code Size, Takehiko Mori, Manabu Hagiwara, IEEE Transaction on Information Theory, Early Access, 2020/08.
DOI: https://doi.org/10.1109/TIT.2020.3016261

誌上発表 和文誌 依頼･招待論文等

JI1) ポストモダン符号理論としてのネットワーク，置換，形式化1:モダン符号理論，萩原学，日本応用数理学会誌 応用数理，26 (1)，pp.33-38，2016.
DOI: https://s://doi.org/10.11540/bjsiam.26.1_33

JI2) ポストモダン符号理論としてのネットワーク，置換，形式化2:ネットワーク符号，萩原学，日本応用数理学会誌 応用数理，26(2)，pp.75-80，2016.
DOI: https://s://doi.org/10.11540/bjsiam.26.2_27

JI3) 誤り訂正符号の例と将来展望，萩原学，映像メディア学会誌 特集「誤り訂正技術 ～基礎編～」，2016 年 7 月号.
DOI: https://s://doi.org/10.3169/itej.70.567

JI4) ポストモダン符号理論としてのネットワーク，置換，形式化3:置換符号，萩原学，日本応用数理学会誌 応用数理，26(3)，pp.125-130，2016.
DOI: https://s://doi.org/10.11540/bjsiam.26.3_29

JI5) ポストモダン符号理論としてのネットワーク，置換，形式化4:符号理論の形式化，萩原学，日本応用数理学会誌 応用数理，26(4)，pp.172-177，2016.
DOI: https://s://doi.org/10.11540/bjsiam.26.4_28

誌上発表 国際シンポジウム Proceeding 学会発行 査読あり

C1) Irregular Low-Density Parity-Check Code Design Based on Euclidean Geometry and Cayley Graph, Wataru MATSUMOTO, Manabu HAGIWARA, Hideki IMAI , Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2002, pp287-290, 2002/10.

C2) An Authentication Scheme for a Quantum Key Distribution using Strongly Universal Hashing , Eguchi Makoto , Hagiwara Manabu , Imai Hideki , Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA)2004, Italy, CD-ROM, 2004/10.

C3) On Minimal Length of Quasi Cyclic LDPC Codes with Girth Greater Than or Equal to 6, Manabu HAGIWARA, Koji Nuida, Takashi Kitagawa, Marc Fossorier, Hideki Imai, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2006, CD-ROM, 2006/10.

C4) Quantum Secure Direct Communication Protocols for Sending a Quantum State, Yumiko Murakami, Masaki Nakanishi, Manabu HAGIWARA, Shigeru Yamashita, Kohsuke Nakajima , Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2006, CD-ROM, 2006/10.

C5) On the Correcting Property of a Two-dimensional Error-correcting Code Based on the Lee Metric on Z_(2^m), Banri Bannai, Manabu HAGIWARA, Hideki Imai, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA)2006, CD-ROM, 2006/10.

C6) Quantum Quasi-Cyclic LDPC Codes, Manabu HAGIWARA, Hideki Imai, Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON INFORMATION THEORY (ISIT) 2007, pp.638-642, 2007/06.

C7) An Efficient Tracing Algorithm for a 2-Secure and Short Random Fingerprint Code, Satoshi Fujitsu, Manabu HAGIWARA, Hideki Imai, Takashi Kitagawa, Koji Nuida, Kazuto Ogawa, Hajime Watanabe, Proceeding of International Workshop on Information Hiding and Digital Watermarking, pp.1-11, 2007/07.

C8) A Quantum Secure Direct Communication Protocol for Sending A Quantum State and Its Security Analysis, Yumiko Murakami, Masaki Nakanishi, Manabu HAGIWARA, Shigeru Yamashita, Yasuhiko Nakashima, Proceeding of the 6th WSEAS International Conference on Information Security and Privacy ,

pp.91-97, 2007/12.

C9) A Group Testing Based Deterministic Tracing Algorithm for a Short Random Fingerprint Code, Takashi Kitagawa, Manabu HAGIWARA, Koji Nuida, Hajime Watanabe, Hideki Imai, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2008, pp.706-710, 2008/12.

C10) A Study on a Key Establishment Scheme with QC LDPC Codes and UH-Protocols, Yuto Matsunaga, Manabu HAGIWARA, Hideki IMAI, Kazuhiko Kobara , Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA)2008, pp.1-6, 2008.

C11) LDPC Codes with Fixed Initialization Decoding over Binary Symmetric Channel, Manabu HAGIWARA, Marc Fossorier, Hideki Imai, Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2010, pp.784-788, 2010/06.

C12) Spatially Coupled Quasi-Cyclic Quantum LDPC Codes, Manabu HAGIWARA, Kenta Kawaii , Hideki Imai , Koichi Sakaniwa , Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2011 , pp.543-547, 2011/07.

C13) LP Decodable Permutation Codes based on Linearly Constrained Permutation Matrices, Tadashi Wadayama, Manabu HAGIWARA, Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2011 , pp.100-105, 2011/07.

C14) Non-Binary Quasi-Cyclic Quantum LDPC Codes, Manabu HAGIWARA, Hideki Imai , Kenta Kasaii , Koichi Sakaniwa , Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2011 , pp.653-657, 2011/07.

C15) Formalization of Shannon's Theorems in SSReflect-Coq, Reynald Affeldt, Manabu Hagiwara, Proceeding of Interactive Theorem Proving (ITP) 2012, 3-249, 2012/08, Springer.

C16) On ML-Certificate Linear Constraints for Rank Modulation with Linear Programming Decoding and its Application to Compact Graphs, Manabu HAGIWARA , Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2012, pp.3003-3007.

C17) Linear Programming Upper Bounds on Permutation Code Sizes From Coherent Configurations Related to the Kendall-Tau Distance Metric, Fabian Lim, Manabu Hagiwara, Proceeding of IEEE INTERNATIONSL SYMPOSIUM ON

INFORMATIONTHEORY (ISIT) 2012, pp.3008-3012.

C18) Comparing Euclidean, Kendall tau Metrics Toward Extending LP Decoding, Justin Kong, Manabu Hagiwara, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2012, pp. 91-95.

C19) Weight Enumerator Analysis for (2, P)- and (3, P)-SFA LDPC Codes, Manabu Hagiwara , James Nation , Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2012, pp. 556-560.

C20) Cryptographic Key Generation from PUF Data Using Efficient Fuzzy Extractors, Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura , Proceeding of International Conference on Advanced Communications Technology (ICACT) 2014, pp.23-26, 2014.

C21) Formalization of the Variable-Length Source Coding Theorem: Direct Part, Ryosuke Obi , Manabu Hagiwara , and Reynald Affeldt , Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2014, Oct., pp.201-205, 2014.

C22) On the Primitive Polynomial as the Characteristic Polynomial of a Symmetric Companion Matrix, Manabu Hagiwara and Takaaki Sasaki, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA)2014, Oct., pp.361-365, 2014.

C23) On Ordered Syndromes for Multi Insertion/Deletion Error-Correcting Codes, Manabu Hagiwara , Proceeding of INTERNATIONSL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2016, July, pp.625-629, 2016.

C24) Nonexistence of Perfect Permutation Codes in the Ulam Metric, Justin Kong and Manabu Hagiwara, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA), pp. 727-731, IEICE, 2016.

C25) Formalization of Coding Theory using Lean, Manabu Hagiwara, Kyosuke Nakano and Justin Kong, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA), pp. 527-531, IEICE, 2016.

C26) A Deep Neural Network Architecture Using Dimensionality Reduction with Sparse Matrices , W. Matsumoto , Manabu Hagiwara , P. T. Boufounos , K. Fukushima, T. Mariyama, Z. Xiongxin, International Conference on Neural Information、Proceedings 2016, pp.397-404, Springer, 2016.

C27) Formalization of Binary Symmetric Erasure Channel Based on Infotheo,

Kyosuke Nakano and Manabu Hagiwara, Proceeding of INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA), pp.512-516, IEICE, 2016.

C28) Perfect codes for single balanced adjacent deletions, Manabu Hagiwara, Proceeding of IEEE INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2017, pp.1938-1942, IEEE, 2017.

C29) Multipermutation Ulam sphere analysis toward characterizing maximal code size, Justin Kong, Manabu Hagiwara, Proceeding of IEEE INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2017, pp.1628-1632, IEEE, 2017.

C30) Descent Moment Distributions for Permutation Deletion Codes via Levenshtein Codes, Manabu Hagiwara, Justin Kong, Proceeding of IEEE INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY (ISIT) 2018, pp.81-85, IEEE, 2018.

C31) Formalization of Insertion/Deletion Codes and the Levenshtein Metric in Lean, Justin Kong, David Webb, Manabu Hagiwara, INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2018, Oct. 2018, pp.1-6, IEICE, 2018.

C32) Cardinalities of BAD Correcting Codes, Takehiko Mori, Manabu Hagiwara, INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA) 2018, pp.13-18, Oct. 2018.

C33) A Four-Qubits Code that is a Quantum Deletion Error-Correcting Code with the Optimal Length, Manabu Hagiwara and Ayumu Nakayama, ISIT 2020, pp.1876-1880, June, 2020.

C34) Conversion Method from Erasure Codes to Multi-Deletion Error-Correcting Codes for Information in Array Design, Manabu Hagiwara, ISITA2020, pp.274-278, Oct. 2020, virtual.

C35) Formalization of VT Codes and Their Single-Deletion Correcting Property in Lean, Yuki Kondo, Manabu Hagiwara, Midori Kudo, ISITA2020, pp.597-601, Oct.2020, virtual.

C36) Decoding Algorithms of Monotone Codes and Azinv Codes and Their Unified View, Hokuto Takahashi, Manabu Hagiwara, ISITA2020, pp.284-288, Oct.2020, virtual.

C37) Single Quantum Deletion Error-Correcting Codes, Ayumu Nakayama, Manabu Hagiwara, ISITA2020, pp.329-333, Oct.2020, virtual.

誌上発表 予稿集・講究録等 査読なし

A1) Minuscule Heaps Over Simply-Laced, Star-shaped Dynkin Diagrams, 萩原学, 数理解析研究所講究録 1262 Young 図形をめぐる話題と表現論, p84-100, 京都大学数理解析研究所, 2001/12.

A2) アフィンワイル群のミヌスクル元, 萩原学, 数理解析研究所講究録 1310 組み合わせ論的表現論とその周辺, pp.1-15 , 2002/11.

A3) On the Turbo-principle in LDPC codes, Manabu Hagiwara, Wataru Matsumoto, Hideki Imai, 第五回「代数幾何・数論及び符号・暗号」研究集会報告集, pp.87-99 , 2004/04.

A4) BB84 量子鍵配送プロトコルの為の双対符号を含む LDPC 符号構成法, 大畑真生, 萩原学, 松浦幹太, 今井 秀樹, 第28回情報理論とその応用シンポジウム 予稿集, I-, pp.411-414, 2005/11.

A5) 復号誤りを利用した量子暗号の為の CSS 型 LDPC 符号構成, 萩原 学, 今井 秀樹, 第28回情報理論とその応用シンポジウム, I-, pp.415-418, 2005/11.

A6) Unconditionally Secure Chaffing-and-Winnowing, 花岡 悟一郎, 花岡 裕都子, 萩原 学, 渡邊 創, 今井秀樹, 第 28 回情報理論とその応用シンポジウム(SITA2005)予稿集, CD-ROM, 2005/11.

A7) Tardos 符号の検証, 藤津智, 萩原 学, 今井 秀樹, 北川 隆, 縫田 光司, 小川一人, 渡邊 創, 第29回情報理論とその応用シンポジウム予稿集, CD-ROM, pp.489-492, 2006/11.

A8) Tardos 符号の解析と追跡アルゴリズムの改良, 藤津智, 萩原 学, 今井 秀樹, 北川 隆, 縫田 光司, 小川一人, 渡邊 創, 第 29 回情報理論とその応用シンポジウム予稿集, pp.493-496, 2006/11.

A9) On a Construction of a Non-stabilier Clifford Quantum Code for 2h(2j+1)-Level States, Manabu HAGIWARA, Hidaki Imai, ELECTRONICS AND COMMUNICATIONS IN JAPAN PART III-FUNDAMENTAL ELECTRONIC SCIENCE, 90-4, pp.63-68, 2006/12.

A10) 2 名の結託攻撃に耐性を有する符号の追跡アルゴリズムの改良, 藤津智, 萩原 学, 今井 秀樹, 北川 隆, 縫田 光司, 小川一人, 渡邊 創, 2007 年暗号と情報セキュリティシンポジウム(SCIS2007)予稿集, CD-ROM, 2007/01.

A11) 記憶容量の観点からの Tardos 符号の最適化, 縫田 光司, 萩原 学, 渡邊 創, 今井秀樹, 2007 年暗号と情報セキュリティシンポジウム(SCIS2007)予稿集, CD-ROM, 2007/01.

A12) On the Key-Privacy Issue of McEliece Public-Key Encryption, 山川 茂紀, Cui

Yang，古原 和邦，萩原 学，今井 秀樹，情報理論とその応用シンポジウム予稿集，CD-ROM，2007/11．

A13) LDPC 符号を用いた可変指向性アンテナを用いた秘密鍵共有システムの雑音除去，松永雄斗，萩原 学，古原 和邦，今井 秀樹，情報理論とその応用シンポジウム予稿集，CD-ROM，2007/11．

A14) 結託耐性ランダム符号のための統計的手法を用いた追跡アルゴリズム，北川 隆，萩原学，縫田 光司，渡邊 創，小川一人，今井 秀樹，2008 年暗号と情報セキュリティシンポジウム 論文集，CD-ROM，2008/01．

A15) 誤り訂正とプライバシー増幅の関係についての検討，松永 雄斗，萩原 学，美添 一樹，古原 和邦，今井 秀樹，SCIS2008 予稿集，CD-ROM，2008/01．

A16) LDPC 符号の各ビット位置のエラー率を求めるシミュレーションの高速化の検討，松永雄斗，萩原 学，今井 秀樹，情報理論研究会技術報告書，CD-ROM，2008/09

A17) Short 3-Secure Random Fingerprint Codes，北川 隆，萩原 学，縫田 光司，渡邊 創，今井 秀樹，2009 年暗号と情報セキュリティシンポジウム予稿集，CD-ROM，2009/01．

A18) LDPC 符号を用いた McEliece 署名方式，山川 茂紀，Cui Yang，萩原 学，古原 和邦，今井 秀樹，IEICE Technical Report，CD-ROM，2009/03．

A19) 情報部の誤り率が小さい LDPC 符号の構成と解析，松永雄斗，萩原 学，今井 秀樹，情報理論とその応用シンポジウム予稿集，CD-ROM，2009/12．

A20) 変数頂点が[7，4]符号により一般化された LDPC 符号の解析，篠永崇史，萩原 学，今井 秀樹，情報理論とその応用シンポジウム予稿集，CD-ROM，2009/12．

A21) 電波伝搬の特性を利用した鍵共有方式の情報量的安全性評価，松永雄斗，吉田 隆弘，萩原 学，古原 和邦，今井 秀樹，SCIS2010予稿集，CD-ROM，2010/01．

A22) 単一ドットを用いた情報付加手法に適した LDPC 符号に関する検討，松原 徳久，萩原学，岩村 恵市，SCIS2010予稿集，CD-ROM，2010/01．

A23) QR コードの改ざんによるフィッシング問題に対して安全な運用及び読み取りプロトコルの提案と安全性検証，篠永 崇史，萩原 学，今井 秀樹，SCIS2010 予稿集，CD-ROM，2010/01．

A24) 量子誤り訂正符号を用いたエンタングルメント蒸留プロトコルの性能評価に関する検討，吉田雅一，萩原 学，宮寺 隆之，今井 秀樹，信学技法，2010/09．

A25) 2 準位量子 QC-LDPC 符号を GF(2)の拡大体の同伴行列で拡張するための十分条件，小柳裕嵩，萩原 学，今井 秀樹，情報理論とその応用学会 予稿集，CD-ROM，2010/12．

A26) Quantum Error Correction with Non-Binary LDPC codes，笠井健太，萩原 学，今井 秀樹，坂庭好一，情報理論とその応用学会予稿集，CD-ROM，2010/12．

A27) デザイン二次元コード，萩原 学，電子情報通信学会誌，94-4，pp.341-343，

2011/04.

A28) 可変長情報源符号化逆定理の形式化，小尾良介，萩原学，山本光晴，SITA2014 予稿集，富山県宇奈月ニューオータニホテル，2014/12.

A29) On formalization of basic geometric topology，Ken'ichi Kuga，Manabu Hagiwara，TPP (Theorem proving and provers for reliable theory and implementations) 2014 報告集，pp.110-114，2015/01.

A30) Coq/SSReflect による二元消失通信路の通信路容量の形式化，中野恭輔，萩原学，SITA2015 予稿集，pp.752-757 岡山県倉敷市下電ホテル，2015/11.

A31) Coq/SSReflect による通信路の同型性の形式化，中野恭輔，萩原学，SITA2016 予稿集，pp.318-323，高山グリーンホテル，2016/12.

A32) Binary Multipermutation Ulam Sphere Analysis，Justin Kong，Manabu Hagiwara，SITA2017 予稿集，pp.1-6，月岡温泉，2017/12.

A33) 単一削除符号の漸近的最大濃度の別証明，山崎大雅，萩原学，SITA2019 予稿集，pp.7-12，霧島国際ホテル，2019/11.

A34) Leveshtein の削除誤り訂正アルゴリズムの一般化，髙橋朋久斗，萩原学，SITA2019 予稿集，pp.13-18，霧島国際ホテル，2019/11.

A35) Lean を用いた Levenshtein 符号と復号アルゴリズムの形式化，近藤裕樹，萩原学，SITA2019 予稿集，pp.19-24，霧島国際ホテル，2019/11.

A36) 二次元削除誤り訂正符号の構成，萩原学，SITA2019 予稿集，pp.1-6，霧島国際ホテル，2019/11.

A37) 単一削除誤りに対する量子誤り訂正符号の構成，中山歩，萩原学，信学技法，vol.119，no.376，IT2019-68，pp.185-189，2020/01.

A38) 角度分解光電子分光法における AI を用いた軌道トモグラフィーの開発， 野崎 美沙，羽生田 聖人，平山 瑠海子，萩原 学，ニ木かおり，日本表面真空学会学術講演会，2020/11.

外部資金等獲得

E1) 京都大学数理解析研究所 長期研究員 300,000 円，研究代表者.

E2) 量子情報技術を頑強にする符号化技術の研究，科学研究費補助金 若手研究(B)，独立行政法人日本学術振興会，3,000,000 円，研究代表者，FY2006-2008.

E3) 二次元コードの研究，株式会社コンタクト，3,000,000 円，研究代表，FY2010.

E4) 京都大学数理解析 共同利用，合宿型セミナー(開催地:栃木県足利市)，「組合せ構造の解析と情報理論への応用」，1,000,000 円，研究代表者，2010/8/6～2010/8/9.

E5) 個々の LDPC 符号が持つ正確な誤り訂正性能評価法の研究，科学研究費補助金 若手研究(B)，独立行政法人日本学術振興会，4,030,000 円，研究代表者，FY2010-2011.

E6) 量子鍵配送方式に関する研究，株式会社 東芝，1,000,000 円，研究代表者，2012/7/1～2013/3/31.

E7) 九州大学マス・フォア・インダストリ研究所(IMI) 共同利用，研究集会 II，「モダン符号理論からポストモダン符号理論への展望」，600,000 円，研究代表者，2013/3/4～2013/3/7.

E8) 数学・数理科学と諸科学・産業との連携研究ワークショップ(上記，「モダン符号理論からポストモダン符号理論への展望」補助金)，文部科学省，150,000 円，運営責任者，FY2012.

E9) モダン符号の形式化，科学研究費補助金基盤研究(B)，独立行政法人日本学術振興会，13,100,000 円，研究代表者，FY2013-2015.

E10) 量子鍵配送方式に関する研究Ⅱ，株式会社 東芝(産業技術総合研究所と千葉大学との3者共同研究)，千葉大学 500，000 円 (全体 1,000,000 円)，千葉大学側 研究代表者，2013/7/1～2014/3/31.

E11) コセット符号化の安全性を最も高める線形符号の解明，科学研究費補助金基盤研究(B)，独立行政法人日本学術振興会，10,790,000 円，研究分担者(受入金額6,110,000 円)，FY2014-2017.

E12) スパース構造化による機械学習の高速化技術の研究開発，三菱電機，500,000 円，研究代表者，2014/9/3-2015/3/15.

E13) 分散協調型機械学習の研究開発，三菱電機，1,600,000 円，研究代表者，2015/9/7-2018/3/15.

E14) 論理的に隙のない情報理論テキストの自動生成，科学研究費補助金挑戦的萌芽，独立行政法人日本学術振興会，3,380,000 円，研究代表者，16K12391，FY2016-FY2018.

E15) 同期誤りを訂正する情報符号化法の開発，科学研究費補助金基盤研究(C)，独立行政

法人日本学術振興会，4,810,000 円，研究分担者（受入金額1,300,000円），16K06336，FY2016-FY2018.

E16) ルート系に付随する数学対象を用いた挿入／削除の考察，科学研究費補助金基盤研究 B，独立行政法人日本学術振興会，12,300,000 円，研究代表者，18H01435，FY2018-FY2020.

E17) 二次元配置された情報の欠損・重複を訂正する削除符号の構成研究，2019 年度キオクシア（旧：東芝メモリ）奨励研究，1,100,000 円，研究代表者，2019/08-2020/03.

E18) 削除チャネルモデルの実用的視点に立った拡張に関する研究，キオクシア株式会社，500,000 円（直接経費 384,500 円），2020/12-2021/3/31

特許（登録済）

P1) 英国特許，GB2433399（登録日 18 March 2009），Quantum key distribution protocol，発明者：今井秀樹，萩原学，江口誠.

P2) 日本国特許，特許第 4555979 号（登録日 2010 年 7 月 30 日），量子鍵配送方式及び暗号通信，発明者：今井秀樹，萩原学，江口誠.

P3) 日本国特許，特許 4700408 号（登録日 2011 年 3 月 11 日），不正流出者検出システム，不正流出検出サーバ，及び不正流出者検出プログラム，発明者：小川一人，花岡悟一郎，萩原学.

P4) 米国特許，US 7，936，883 B2 (登録日 May 3，2011)，QUANTUM KEY DISTRIBUTION PROTOCOL，発明者：今井秀樹，萩原学，江口誠.

P5) 日本国特許，特許第 4941912 号（登録日 2012 年 3 月 9 日），符号データ特定装置及びそのプログラム，並びに，フィンガープリント検出装置及びそのプログラム，発明者：小川一人，藤津智，縫田光司，萩原学，北川隆，渡邊創.

P6) 日本国特許，特許第 5110596 号 (登録日 2012 年 12 月 26 日)，二次元コード生成装置，発明者：萩原学，大塚玲.

P7) 日本国特許，特許第 5429909 号（登録日 2013 年 12 月 13 日），二次元コード生成装置により生成される二次元コード，発明者：萩原学，大塚玲.

P8) 日本国特許，特許第 6598259 号（登録日 2019 年 10 月 11 日），デバイス固有情報生成装置及びデバイス固有情報生成システムとデバイス固有情報生成方法，発明者：堀洋平，萩原学，姜玄浩，古原和邦，片下敏宏.

口頭発表 招待･依頼講演 国際

II1) 招待講演，Error-Correcting Codes and Cryptography，今井 秀樹，萩原 学，非筆頭，HISC2006，奈良県，2006/05/24.

II2) 依頼講演，Practical Non dual containing Classical Error Correcting Codes for Quantum Key Distribution，萩原 学，北川 隆，今井 秀樹，筆頭･登壇，XI International Conference on Quantum Optics，Belarus，2006/05/31.

II3) 依頼講演，Quantum Error Correction Code，萩原 学，筆頭･登壇，Summer School on Mathematical Aspects of Quantum Computing，近畿大学，2007/08/27.

II4) 依頼講演，Introduction to Combinatorics of Deletion Codes，萩原学，上海大学理学系 数学院 学术，2019/10/17.

口頭発表 招待・依頼講演 国内

ID1) 依頼講演 事前線形符号化量子符号の符号化と復号，萩原学，第 31 回 QC-North，北海道大学，2004/11/11.

ID2) 依頼講演 量子暗号を頑健にする古典符号技術のLDPC符号による実現，萩原 学，筆頭・登壇，第6回代数幾何・数論及び符号・暗号研究集会，東京大学，2006/01/27.

ID3) 依頼講演 A construction of LDPC code to make QKD stout，萩原 学，筆頭・登壇，ERATO QCI セミナー，東京，2006/01/27.

ID4) 依頼講演 量子暗号の安全性をめぐって，萩原 学，筆頭・登壇，奈良先端大学講義，奈良先端大学，2006/06/05.

ID5) 依頼講演 情報セキュリティ研究におけるLDPC符号の位置，萩原 学，筆頭・登壇，LDPC符号ワークショップ，神奈川県，2006/08/31.

ID6) 依頼講演 量子暗号の基礎と現状，萩原 学，筆頭・登壇，中村研究室セミナー，千葉，2006/09/02.

ID7) 依頼講演 量子情報理論の組合せ論的手法，萩原 学，筆頭・登壇，組合せ理論とその情報科学への応用，京都，2006/09/15.

ID8) 依頼講演 量子ポーラ符号構成の困難性，萩原 学，筆頭・登壇，坂庭研究室セミナー，東京工業大学，2010/10/27.

ID9) 依頼講演 誤り訂正符号を用いた量子力学的性質の保護，萩原 学，筆頭・登壇，諸分野との協働による数理科学のフロンティア，京都大学，2010/11/17.

ID10) 依頼講演 線形計画法，グラフ，置換群，および長さ関数と関連する誤り訂正符号，萩原 学，筆頭・登壇，組合せ論セミナー，東北大学，2012/05/29.

ID11) 依頼講演 Graph theoretic approach to rank modulations and permutation codes，萩原 学，筆頭・登壇，代数的組合せ論シンポジウム，弘前大学，2012/06/19.

ID12) 依頼講演 PUF の概念と評価，そして Fuzzy Extractor による鍵生成，姜 玄浩（東京理科大），萩原 学，誤り訂正符号のワークショップ，沖縄県宜野湾市，2013/09/26.

ID13) 依頼講演 モダン代数的符号と呼ばれるネットワーク誤り訂正符号，萩原学，京都大学数理解析研究所 共同研究「デザイン，符号，グラフおよびその周辺」，2014/7/24.

ID14) 招待講演 萩原学，疎構造やモダン符号の形式化で感じた組合せ論への期待，組合せ論サマースクール 2014，山口県湯田温泉，2014/09/04.

ID15) 依頼講演 萩原学，Gabidulin 符号，誤り訂正符号のワークショップ，千葉県館山市，2014.

ID16) 依頼講演 萩原学，符号理論の形式化入門，名古屋工業大学，2015/3.

ID17) 依頼講演 萩原学，置換符号，誤り訂正符号のワークショップ，石川県加賀市，2015/9/3.

ID18) 依頼講演 萩原学，多重挿入／削除誤り訂正符号の構成と表現，研究集会「実験計画法と符号および関連する組合せ構造」，神奈川県箱根水明荘，2015/12/3.

ID19) 依頼講演，挿入削除誤り訂正符号の数学的に綺麗な性質について，萩原学，電子情報通信学会ソサイエティ大会，東京都市大学，2017/9/13.

ID20) 依頼講演，電子情報通信と数学 ～基礎･境界の視点から～，萩原学，電子情報通信学会総合大会，早稲田大学，2019/3/20.

ID21) 依頼講演，挿入削除符号入門講義，萩原学，株式会社 SONY，2019/6/14，9/6，12/13.

ID22) 招待講演，情報セキュリティへの符号理論の応用，萩原学，日本応用数理学会 2019年度年会 FAIS オーガナイズド･セッション，2019/9/3.

口頭発表 国際会議等 査読あり 予稿無し

OR1) Minuscule Heaps Over Simply-Laced, Star-shaped Dynkin Diagrams, Manabu Hagiwara, FPSAC2002, Melbourne, 2002/07/10

OR2) Non-stabilizer Clifford codes, Manabu HAGIWARA, Hideki IMAI, MS+S2004 (International Symposium on Mesoscopic Superconductivity and Spintronics 2004), NTT R&D Center, Atsugi, Kanagawa, Japan, 2004/03/02

OR3) A tracing algorithm for short 2-secure probabilistic fingerprinting codes strongly protecting innocent users, Koji Nuida, Manabu HAGIWARA, Takashi Kitagawa, Wataru Watanabe, Kazuto Ogawa, Satoshi Fujitsu, Hideki Imai, 3rd IEEE International Workshop on Digital Rights Management (CONSUMER COMMUNICATIONS & NETWORKING CONFERENCE (CCNC) 2007 Satellite Workshop), Nevada, USA, 2007/01/11

OR4) Lattice path enumeration for 321-avoiding permutations with further restrictions, Manabu HAGIWARA, Manabu Inuma, Masaya Tomie, 7th International Conference on Lattice Path Combinatorics and Applications, Italy, 2010/07/05

ロ頭発表 国際会議等 査読なし

OI1) Graphical construction of permutation code，萩原 学，American Mathematics Society，Western Sectional Meeting，Hawaii，USA，2012/03/03.

OI2) Shifted Young diagrams and binary I/D error-correcting codes，Manabu Hagiwara，SIAM DM16，Georgia state，USA，2016/06/07.

OI3) Perfect Codes for BADs and Other Two Deletions，Manabu Hagiwara，Math Seminar，National Taiwan University，2017/08/02.

OI4) Algebraic and Combinatorial Aspects of Insertion/Deletion Operations，Manabu Hagiwara，Lie Seminar，Department of Mathematics，Colorado University，2018/06/26.

OI5) Levenshtein's Deletion Codes and Weyl Groups，Manabu Hagiwara，Seminar at School of Physical and Mathematical Sciences，Nanyang Technological University，2018/10/26.

OI6) Weyl groups and perfect codes for generalized deletions，Manabu Hagiwara，American Mathematical Society Sectional Meeting，University of Hawaii，2019/3/23.

OI7) An Introduction to How to Relate Coding Theory and d-complete Posets，Manabu Hagiwara，AMS and MAA Joint Mathematics Meetings (JMM) 2020，Denver，USA，2020/1/17.

ロ頭発表 国内シンポジウム等 査読なし

OD1) On the length function of the symmetric group relative to the generators of affine type，萩原学，短期共同研究「Young 図形と対称関数をめぐる組合せ論と表現論」，京都大学，1999/10/26.

OD2) Minuscule Heap について--- 特に有限 Weyl 群と星型 Dynkin に関連する Weyl 群の場合 ---，萩原学，研究集会「組合せ論・表現論とその周辺」，岡山大学，2001/01/09.

OD3) 量子誤り訂正符号の研究動向，萩原学 今井秀樹，Designs，Codes，Graphs and their Links，京都大学数理解析研究所，2002/09/04.

OD4) LDPC符号にみるターボ原理，今井秀樹，松本渉，萩原学，第5回代数幾何・数論及び符号・暗号研究集会，東京大学，2003/01/18.

OD5) 量子暗号``吾妻-番プロトコル''プロトコルに用いる特定位置誤り訂正符号に対するグラフ符号の利用，萩原学，今井秀樹，暗号と情報セキュリティシンポジウム，静岡県アクトシティ，2003/01/28.

OD6) 暗号理論の最新の動向 ～量子ワンタイムパッドの研究～，今井秀樹，萩原学，符号と暗号の代数的数理，京都大学，2003/11/04

OD7) 量子鍵配送のための安全な認証法について，江口誠，萩原学，今井秀樹，第９回量子情報技術研究会(QIT9)，NTT 厚木研究開発センタ，2003/12/12.

OD8) 量子ワンタイムパッドに用いる作用素数に関する線形代数的アプローチ，萩原学，今井秀樹，第 26 回情報理論とその応用シンポジウム (SITA2003)，兵庫県立淡路夢舞台国際会議場，2003/12/15.

OD9) 量子鍵配送のための安全な認証法について，暗号と情報セキュリティシンポジウム，江口誠，萩原学，今井秀樹，ホテル仙台プラザ，2004/01/27.

OD10) 量子鍵配送における古典的安全性とノイズ率による鍵生成率評価，萩原学，今井秀樹，SCIS2004，ホテル仙台プラザ，2004/01/27.

OD11) 量子鍵配送における古典的安全性とノイズ率によるか鍵生成率評価，萩原学 今井秀樹，量子情報通信と量子ナノデバイスに関するシンポジウム，東京，2004/03/11.

OD12) 表現論的符号理論 ～ 量子誤り訂正符号 ～，萩原学，組合せ論ヤングサマーセミナー2004/08.

OD13) 光子数分割攻撃に対してより頑強な量子鍵配送プロトコルの提案，江口誠，萩原学，今井秀樹，QIT11，京都大学，2004/12/06.

OD14) 量子鍵配送の光子分割攻撃に対する頑強性と古典通信量の比較，江口誠，萩原学，今井秀樹，第 27 回情報理論とその応用シンポジウム (SITA2004)，岐阜県，2004/12/14.

OD15) グラフを用いた量子符号の符号空間および符号化器，萩原学，今井秀樹，第 27 回情

報理論とその応用シンポジウム (SITA2004)，岐阜県，2004/12/16.

OD16) BB84 プロトコルの量子通信路雑音に対する CSS 型の原始 BCH 符号構成，江口誠，萩原学，今井秀樹，SCIS2005，兵庫県，2005/01/28.

OD17) 4状態を用いた量子鍵配送プロトコルの光子数分割攻撃に対する安全性について，江口誠，萩原学，今井秀樹，SCIS2005，兵庫県，2005/01/28.

OD18) 短距離量子暗号システムにおける安全な誤り訂正符号の構成，萩原 学，今井 秀樹，暗号と情報セキュリティシンポジウム，広島，2006/01/18.

OD19) 低重み符号語探索問題を利用した半正則 CSS-LDPC 符号の設計と量子鍵配送への応用，萩原 学，今井 秀樹，情報理論とその応用シンポジウム，北海道，2006/11/30.

OD20) LDPC 符号を用いた McEliece 公開鍵暗号系の安全性，萩原 学，古原 和邦，今井秀樹，暗号と情報セキュリティシンポジウム，長崎，2007/01/24.

OD21) 非正則疑似巡回低密度パリティ検査符号の量子符号化にまつわる組合せ論的アプローチ，萩原 学，組合せ論サマースクール2007，沖縄県，2007/09/04.

OD22) ねじれ関係にある LDPC 符号の組の構成 ，萩原 学，今井 秀樹，第 30 回 情報理論とその応用シンポジウム，三重県志摩市阿児町賢島，2007/11/27.

OD23) 結託耐性符号の追跡アルゴリズムとしてのグループテスト法とそれに対する攻撃不可能性，萩原 学，北川 隆，今井 秀樹，SCIS2008，宮崎県，2008/01/23.

OD24) 準巡回低密度パリティ検査符号にまつわる離散数学的側面と量子符号への拡張にまつわる問題，萩原 学，COS08，沖縄県，2008/09/09.

OD25) 準巡回 LDPC 行列を利用した結託耐性符号追跡アルゴリズムの検討，北川 隆，萩原学，LDPC 符号ワークショップ，沖縄県宜野湾市，2008/09/12.

OD26) LDPC 符号の訂正可能誤りならびにワード誤り率の導出とその応用，萩原 学，SITA 2009，山口県，2009/12/10.

OD27) 二元対称通信路上の Sum-Product 復号の解析と改良，萩原 学，第4回 高密度記録のための信号処理ワークショップ，愛知県，2010/04/02.

OD28) 量子誤り訂正符号を用いたエンタングルメント蒸留プロトコルの性能評価に関する検討，，吉田雅一，萩原 学，宮寺 隆之，今井 秀樹，LDPC 符号ワークショップ，東北学院大学，2010/09/22.

OD29) ポーラ符号から構成する量子誤り訂正符号の検討，萩原 学，森立平，田中利幸，今井 秀樹，SITA2010，長野，2010/12/02.

OD30) 空間結合構造を持つ量子 LDPC 符号，萩原 学，第 1 回空間結合符号とその周辺ワークショップ，東京工業大学，2011/02/19.

OD31) シャノンの定理の形式化，Affeldt Reynald，萩原 学，日本応用数理学会 2012 年春の研究部会連合発表会，九州大学，2012/03/08.

OD32) SFA-LDPC 符号の同値性，萩原学，J.B.Nation，SITA2013，神奈川県伊東ホテル聚楽，2013/11/27.

OD33) Gabidulin 符号と有限体の構造，萩原学，誤り訂正符号のワークショップ，千葉県館山市，2014/9/18.

OD34) 可変長情報源符号化定理の形式化の改良，萩原学，小尾良介，SITA2014，富山県宇奈月ニューオータニホテル，2014/12/11.

OD35) 順序のある代数系上の挿削除誤り訂正符号，萩原学，SITA2015，岡山県倉敷市下電ホテル，2015/11.

OD36) 多重挿入／削除誤り訂正符号の順序付代数による構成とその表現，萩原学，琉球大学理学部セミナー，2015/12/4

OD37) C 型ルート系に付随する挿入削除誤り訂正符号，萩原学，SITA2016，高山グリーンホテル，2016/12.

OD38) ワイル群のミヌスクル元からの挿入／削除の拡張，萩原学，2017 年度 RIMS 共同研究「表現論と組合せ論」，京都大学，2017/10.

OD39) 入門講義・挿入／削除符号へ誘う綺麗な構造，萩原学，実験計画法と符号および関連する組合せ構造，神奈川県湯河原町，2017/11/24.

委員歴

2015年6月 – 2017年5月

電子情報通信学会 基礎境界ソサイエティ 幹事（特別委員）

2016年3月～2017年10月

国際論文誌 IEICE ISITA 2016 Special Edition，Associate Editor

2017 年 6 月 – 2019 年 6 月

電子情報通信学会 基礎境界ソサイエティ 幹事（電子広報担当）

2017 年 6 月 – 現在

電子情報通信学会 情報理論研究専門委員会 専門委員

2017 年 6 月 – 現在

電子情報通信学会 和文論文誌A編集委員会 和文論文誌編集委員

2017 年 8 月 – 2018 年 7 月

日本学術振興会 卓越研究員候補者選考 審査員

2017年10月～2018年10月

国際論文誌 IEICE ISITA 2018 Special Edition，Associate Editor

2017 年 – 現在

国際シンポジウム INTERNATIONAL SYMPOSIUM ON INFORMATIONTHEORY AND ITS APPLICATIONS (ISITA)2020 実行委員会 実行委員長

2018 年5月 – 2020年 5 月

電子情報通信学会 情報理論とその応用サブソサイエティ 委員（庶務担当）

教育実績　講義

2013年～現在

千葉大学 理学研究院（旧：理学研究科）

准教授（2013 年 4 月～2020 年 5 月）

教授　（2020 年 6 月～現在）

担当講義：情報学演習，符号理論，情報数理学特論 I，情報数学2，数学・情報数理学基礎セミナー，応用情報数理学特論，現代応用情報数理学

非常勤講師として：

2009年度

横浜国立大学大学院環境情報学府	数理・論理セキュリティ（うち1コマ）

2010年度

千葉大学理学部数学・情報数理学科	情報学演習

2013年度

九州大学マス・フォア・インダストリ研究所	数理科学特論5

2014年度

名古屋大学大学院多元数理科学研究科	代数学特別講義 IV
東京女子大学 数理科学科	符号と暗号 A

2014年度～現在

中央大学 大学院 理工学研究科	符号理論特論

2016年度

お茶の水女子大学 大学院人間文化創生科学研究科	応用代数学特論

2017年度

山口大学 理学部物理・情報科学科	情報科学特別講義：符号理論概論

一般雑誌等

M1）数理科学「符号化理論の研究動向」「量子誤り訂正符号」，萩原学，サイエンス社，2004年 11 月号.

M2）数学セミナー「通信路符号化」，萩原学，日本評論社，2006 年 10 月号.

M3）数学セミナー2007 年 8 月号「エレガントな解答を求む（出題編）」，2007 年 11 月号「エレガントな解答を基む（解答編）」，萩原学，日本評論社.

M4）数学セミナー，連載「アキバ道研究屋稼業」，萩原学，日本評論社，2008 年 4 月号～2009 年 3 月.

M5）数学セミナー「探偵助手」（萩原学・小林泰三・平野美子），萩原学，日本評論社，2009年 4 月号.

M6）数学セミナー「解けそうで解けない数学の問題～差行列の理論と現代符号理論の境界問題」，萩原学，日本評論社，2009 年 9 月号.

M7）数学セミナー，リレー連載「ふごζXう」，萩原学，日本評論社，2012 年 7 月号～2013年 6 月号.

M8) 数学セミナー，連載「萩原学のキネマの数学」，萩原学，日本評論社，2019 年 4 月号～2021 年 3 月号（全24回）.