研究業績リスト

2016年6月２２日現在

件数一覧

・著作等（書籍２件、雑誌７件）
・誌上発表（査読あり国際誌　１９件，査読あり和文誌　２件，依頼・招待論文和分誌　３件，査読あり予稿集　２４件，査読なし講究録等　４３件）
・外部資金等　１９件
・特許７件
・口頭発表（招待・依頼講演　国際 ３件，招待・依頼講演 国内　１８件，国際（査読あり）34件，国際（査読無し）１件，国内（査読なし）６２件）
・受賞　１件（共著）

書籍 ２冊

著 1） 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

著 2） 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～」, 日本評論社, 2012/8/10 発刊

雑誌 ７編

雑 1） 数理科学「符号化理論の研究動向」「量子誤り訂正符号」, サイエンス社, 2004 年 11 月号.

雑 2） 数学セミナー「通信路符号化」, 日本評論社, 2006 年 10 月号.

雑 3） 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)」, 日本評論社 .

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

雑 5） 数学セミナー「探偵助手」(萩原学・小林泰三・平野美子), 日本評論社, 2009 年 4 月号.

雑 6） 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」, 日本評論社, 2009 年 9 月号.

雑 7） 数学セミナー, リレー連載「ふごξ×う」, 日本評論社, 2012 年 7 月号～2013 年 6 月号.

誌上発表（査読あり国際誌 19 編，査読あり和文誌 2 編，
依頼・招待論文和分誌３編，
査読あり予稿集２４編，査読なし講究録等４３編）

誌上発表 国際誌 査読あり

A1) Minuscule Heaps over Dynkin Diagrams of Type ¥tilde A, Manabu Hagiwara, The Electronic Journal of Combinatorics, vol. 11 (2004), R3, 20pp，2004/01.

A2) A characterization of the simply-laced FC-finite Coxeter groups, Manabu HAGIWARA, Masao ISHIKAWA, Hiroyuki TAGAWA, Annals of Combinatorics, pp.177-196，2004/08.

A3) A Construction for Non-Stabilizer Clifford Code, Manabu HAGIWARA, Hideki IMAI, REALIZING CONTROLLABLE QUANTUM STATES, pp.304-309，2005/11.

A4) A Short Random Fingerprinting Code against a Small Number of Pirates，Manabu HAGIWARA，Goichiro Hanaoka，Hideki Imai，LECTURE NOTES IN COMPUTER SCIENCE，3857，pp.193-202，2006/02.

A5) Unconditionally Secure Chaffing-and-Winnowing: A Relationship between Encryption and Authentication, Goichiro Hanaoka, Yumiko Hanaoka（NTT ドコモ），Manabu HAGIWARA，Hajime Watanabe，Hideki Imai，LECTURE NOTES IN COMPUTER SCIENCE，3857，pp.154-162，2006/02.

A6) On the Key-Privacy Issue of McEliece Public-Key Encryption，Shigeki Yamakawa（中央大学），Cui Yang，Kazukuni Kobara，Manabu HAGIWARA，Hideki Imai，Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes，LNCS4851，pp.168-177，2007/12.

A7) An Improvement of Tardos's Collusion-Secure Fingerprinting Codes with Very Short Lengths，Koji Nuida，Satoshi Fujitsu（NHK 放送技術研究所），Manabu HAGIWARA，Takashi Kitagawa，Hajime Watanabe，Kazuto Ogawa（NHK 放送技術研究所），Hideki Imai, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes，LNCS4851，pp.80-89，2007/12.

A8) Optimization of Tardos's Fingerprinting Codes in a Viewpoint of Memory Amount，Koji Nuida，Manabu HAGIWARA，Hajime Watanabe，Hideki Imai，Hideki Imai，Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes，LNCS4567，

pp.279-293，2008/01.

A9) Error-correcting codes and cryptography，Hideki Imai，Manabu HAGIWARA，APPLICABLE ALGEBRA IN ENGINEERING COMMUNICATION AND COMPUTING，19-3，pp.213-228，2008/04.

A10) An Efficient 2-Secure and Short Random Fingerprint Code and its Security Evaluation，Koji Nuida，Satoshi Fujitsu（NHK 放送技術研究所），Manabu HAGIWARA，Hideki Imai，Takashi Kitagawa，Kazuto Ogawa（NHK 放送技術研究所），Hajime Watanabe，IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS COMMUNICATIONS AND COMPUTER SCIENCES，92-1，pp.197-206，2009/01.

A11) An improvement of discrete Tardos fingerprinting codes，Koji Nuida，Satoshi Fujitsu（NHK 放送技術研究所），Manabu HAGIWARA，Takashi Kitagawa，Hajime Watanabe，Kazuto Ogawa（NHK 放送技術研究所），Hideki Imai，DESIGNS CODES AND CRYPTOGRAPHY，Vol.52, 3，pp.339-362，2009/04.

A12) Bounds on the Number of Users for Random 2-Secure Codes，Manabu HAGIWARA，Takahiro Yoshida（中央大学），Hideki Imai，Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes，LNCS 5527，pp.239-242，2009/06.

A13) Smallest Size of Circulant Matrix for Regular Quasi-Cyclic LDPC Codes with Girth at Least 6，Manabu HAGIWARA，Takashi Kitagawa，Marc Fossorier（ENSEA），Hideki Imai，IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES，E92-A-11，pp.2891-2894，2009/11.

A14) Quantum Error Correction Beyond the Bounded Distance Decoding Limit，Kenta Kasai（東京工業大学），Manabu HAGIWARA，Hideki Imai，Koichi Sakaniwa（東京工業大学），IEEE TRANSACTIONS ON INFORMATION THEORY，58-2，pp.1223-1230，2012/02.

A15) Fixed Initialization Decoding of LDPC codes over a Binary Symmetric Channel，Manabu HAGIWARA，Marc Fossorier（ENSEA），Hideki Imai，IEEE TRANSACTIONS ON INFORMATION THEORY，58-4，pp.2321-2329，2012/04.

A16) LP Decodable Permutation Codes based on Linearly Constrained Permutation Matrices, Tadashi Wadayama, Manabu Hagiwara, IEEE TRANSACTIONS ON INFORMATION THEORY, 58-8, pp.5454-5470, 2012/8.

A17) 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, 2012/09.

A18) Reynald Affeldt, Manabu Hagiwara, and Jonas Sénizergues. Formalization of Shannon's Theorems, Journal of Automated Reasoning, 53(1), pp.63-103, 2014, Springer.

A19) Manabu Hagiwara, A short proof for the multi-deletion error correction property of Helberg codes, IEICE Communications Express, Vol.5 (2016) No.2, pp.49-51, DOI: http://doi.org/10.1587/comex.2015XBL0182

誌上発表 和文誌 査読あり

B1) 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.

B2) 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.

誌上発表 和文誌 依頼・招待論文

B' 1) 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， 1 号, 2016.

B' 2) 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， 2 号, 2016.

B' 3) 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.

誌上発表 Proceedings 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, Proc. of 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, Proc. of ISITA2004, 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 (Univ. of Hawaii), Hideki Imai, Proc. of ISITA 2006, CD-ROM, 2006/10.

C4) Quantum Secure Direct Communication Protocols for Sending a Quantum State, Yumiko Murakami (NAIST), Masaki Nakanishi (NAIST), Manabu HAGIWARA, Shigeru Yamashita (NAIST), Kohsuke Nakajima (NAIST), Proc. of 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 (東京大学), Manabu HAGIWARA, Hideki Imai, Proc. of ISITA2006, CD-ROM, 2006/10.

C6) A tracing algorithm for short 2-secure probabilistic fingerprinting codes strongly protecting innocent users, Koji Nuida, Manabu HAGIWARA, Takashi Kitagawa, Hajime Watanabe, Kazuto Ogawa (NHK 放送技術研究所), Satoshi Fujitsu (NHK 放送技術研究所), Hideki Imai, Proc. of IEEE CCNC 2007, 2007/01.

C7) Quantum Quasi-Cyclic LDPC Codes, Manabu HAGIWARA, Hideki Imai, Proc. of IEEE ISIT 2007, pp.638-642, 2007/06.

C8) An Efficient Tracing Algorithm for a 2-Secure and Short Random Fingerprint Code, Satoshi Fujitsu (NHK 放送技術研究所), Manabu HAGIWARA, Hideki Imai, Takashi Kitagawa, Koji Nuida, Kazuto Ogawa (NHK 放送技術研究所), Hajime Watanabe, Proc. of International Workshop on Information Hiding and Digital Watermarking (IWIHDW 2007), pp.1-11, 2007/07.

C9) A Quantum Secure Direct Communication Protocol for Sending A Quantum State and Its Security Analysis, Yumiko Murakami (Mitsubishi Electric Corporation), Masaki Nakanishi (Nara Institute of Science and Techonology), Manabu HAGIWARA, Shigeru Yamashita (Nara Institute of Science and Technology), Yasuhiko Nakashima (Nara Institute of Science and Technology), Proc. of the 6th WSEAS International Conference on Information Security and Privacy, pp.91-97, 2007/12.

C10) A Group Testing Based Deterministic Tracing Algorithm for a Short Random Fingerprint Code, Takashi Kitagawa, Manabu HAGIWARA, Koji Nuida, Hajime Watanabe, Hideki Imai, Proc. of ISITA 2008, pp.706-710, 2008/12.

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

C12) Spatially Coupled Quasi-Cyclic Quantum LDPC Codes, Manabu HAGIWARA, Kenta Kawaii（東京工業大学), Hideki Imai, Koichi Sakaniwa（東京工業大学), Proc. of IEEE ISIT 2011, pp.543-547, 2011/07.

C13) LP Decodable Permutation Codes based on Linearly Constrained Permutation Matrices, Tadashi Wadayama (名古屋工業大学), Manabu HAGIWARA, Proc. of IEEE ISIT 2011, pp.100-105, 2011/07.

C14) Non-Binary Quasi-Cyclic Quantum LDPC Codes, Manabu HAGIWARA, Hideki Imai, Kenta Kasaii (東京工業大学), Koichi Sakaniwa (東京工業大学), Proc. of IEEE ISIT 2011, pp.653-657, 2011/07.

C15) Formalization of Shannon's Theorems in SSReflect-Coq, Reynald Affeldt, Manabu Hagiwara, Proc. of Interactive Theorem Proving 2012 (ITP2012), pp.233-249, 2012/08, Springer.

C16) On ML-Certificate Linear Constraints for Rank Modulation with Linear Programming Decoding and its Application to Compact Graphs, Manabu HAGIWARA, Proc. of IEEE 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 (MIT), Manabu Hagiwara, Proc. of IEEE ISIT 2012, pp.3008-3012.

C18) Comparing Euclidean, Kendall tau Metrics Toward Extending LP Decoding, Justin Kong (Univ. of Hawaii), Manabu Hagiwara, Proc. of ISITA 2012, pp. 91-95.

C19) Weight Enumerator Analysis for (2,P)- and (3,P)-SFA LDPC Codes, Manabu Hagiwara, James Nation (Univ. of Hawaii), Proc. of ISITA 2012, pp. 556-560.

C20) 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, pp.277-284, 2014.

C21) Cryptographic Key Generation from PUF Data Using Efficient Fuzzy Extractors, Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura Proc. of ICACT 2014, pp.23-26, 2014.

C22) Ryosuke Obi, Manabu Hagiwara, and Reynald Affeldt, Formalization of the Variable-Length Source Coding Theorem: Direct Part, Proc. of ISITA2014, Oct.,

pp.201-205, 2014.
C23) Manabu Hagiwara and Takaaki Sasaki, On the Primitive Polynomial as the Characteristic Polynomial of a Symmetric Companion Matrix, Proc of ISITA2014, Oct., pp.361-365, 2014.
C24) Manabu Hagiwara, On Ordered Syndromes for Multi Insertion/Deletion Error-Correcting Codes, Proc. of ISIT2016, July., accepted, 2016.

誌上発表 査読なし

D1) 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.

D2) 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.

D3) 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.

D4) 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（東京大学), 萩原 学, 松浦幹太（東京大学), 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, 1-, pp.411-414, 2005/11.

D5) 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, 1-, pp.415-418, 2005/11.

D6) Unconditionally Secure Chaffing-and-Winnowing, 花岡 悟一郎, 花岡 裕都子（NTT ドコモ), 萩原 学, 渡邊 創, 今井秀樹（東大/情報セキュリティ研究センター), 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.

D7) 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 2006 予稿集, CD-ROM, 2006/01.

D8) 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, 第６回代数幾何・数論及び符号・暗号研究集会, 予稿集, 2006/04.

D9) Practical Non dual containing Classical Error Correcting Codes for Quantum Key Distribution, Manabu HAGIWARA, Takashi Kitagawa, Hideki Imai, Proc. of ICQO 2006, 2006/05.

D10) Tardos 符号の検証, 藤津智（日本放送協会 放送技術研究所), 萩原 学, 今井 秀樹, 北川 隆, 縫田 光司, 小川一人（日本放送協会 放送技術研究所), 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.

D11) Tardos 符号の解析と追跡アルゴリズムの改良, 藤津智（日本放送協会 放送技術研究所), 萩原 学, 今井 秀樹, 北川 隆, 縫田 光司, 小川一人（日本放送協会 放送技術研究所), 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.

D12) 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.

D13) 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（日本放送協

会　放送技術研究所)，萩原 学，今井 秀樹，北川 隆，縫田 光司，小川一人（日本放送協会　放送技術研究所)，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.

D14) 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.

D15) A short random fingerprint code and its tracing algorithm which uses group testing ，Takashi Kitagawa，Manabu HAGIWARA，2007 Hawaii and SITA Joint Conference on Information Theory, pp.78-82，2007/05.

D16) On the Key-Privacy Issue of McEliece Public-Key Encryption，山川 茂紀（中央大学理工学部)，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.

D17) 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（中央大学)，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.

D18) 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予稿集，CD-ROM，2007/11.

D19) 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（NHK 放送技術研究所)，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.

D20) 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（中央大学)，萩原 学，美添 一樹（中央大学)，古原 和邦，今井 秀樹，SCIS2008 予稿集，CD-ROM，2008/01.

D21) 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，2008 年 暗号と情報セキュリティシンポジウム予稿集，CD-ROM，2008/01.

D22) 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（中央大学)，萩原 学，今井 秀樹，情報理論研究会技術報告書，CD-ROM，2008/09

D23) 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.

D24) LDPC 符号を用いた McEliece 署名方式，山川 茂紀（中央大学理工学部)，Cui Yang，萩原 学，古原 和邦，今井 秀樹，IEICE Technical Report，CD-ROM，2009/03.

D25) 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，情報理論とその応用シンポジウム予稿集，CD-ROM，2009/12.

D26) 情報部の誤り率が小さい LDPC 符号の構成と解析，松永雄斗（中央大学)，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.

D27) 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（中央大学)，

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.

D28) 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（中央大学)，吉田 隆弘，萩原 学，古原 和邦，今井 秀樹，ＳＣＩＳ２０１０予稿集，CD-ROM，2010/01.

D29) 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（東京理科大学)，萩原 学，岩村 恵市，ＳＣＩＳ２０１０予稿集，CD-ROM，2010/01.

D30) 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.

D31) 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（中央大学)，萩原 学，宮寺 隆之，今井 秀樹，信学技法，2010/09.

D32) 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（京都大学)，田中利幸（京都大学)，今井 秀樹，情報理論とその応用学会予稿集，CD-ROM，2010/12.

D33) 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，小栁裕嵩（中央大学)，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.

D34) Quantum Error Correction with Non-Binary LDPC codes，笠井健太（東京工業大学)，萩原 学，今井 秀樹，坂庭好一（東京工業大学)，情報理論とその応用学会予稿集，CD-ROM，2010/12.

D35) 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.

D36) 誤り訂正符号を用いた量子力学的性質の保護 –量子誤り訂正符号入門- 萩原学，数理解析研究所講究録 1752 諸分野との協働による数理科学のフロンティア，p7-21，京都大学数理解析研究所，2011/7.

D37) SFA-LDPC 符号の同値性，萩原学, J.B.Nation, SITA2013 予稿集，神奈川県伊東ホテル聚楽, pp.163-168, 2013/11.

D38) 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.

D39) 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 予稿集，富山県宇奈月ニューオータニホテル, 2014/12.

D40) 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講究録, 1659, pp.75-93, (2015).

D41) 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.

D42) 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.

D43) 順序のある代数系上の挿削除誤り訂正符号, 萩原学, SITA2015 予稿集, pp.469-474, 岡山県倉敷市下電ホテル, 2015/11.

外部資金獲得および企業との共同研究　１９件

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. 量子暗号技術の研究開発，NEC（日本電気），三菱電機，東京大学の３社共同研究（東京大学側として参加），2002 年度～2005 年度，(TAO からの委託研究)，３社計 2002 年度 150,000,000 円,2003 年度 187,500,000 円，2004 年度 189,000,000 円，2005 年度 180,000,000 円，研究協力者.

E3. 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.

E4. コンテンツ配信フィンガープリント方式の研究，NHK 放送技術研究所，2006 年度～2008 年度，研究代表者.

E5. 日本―印度研究交流,「RFID とセンサネットワーク向け暗号基礎技術とそれを用いた構成要素の設計および安全性評価」，2008 年 12 月～2013 年 3 月，24,086,999 円，研究協力者.

E6. 二次元コードの研究，株式会社コンタクト，2010 年度，　3,000,000 円

E7. 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」，2010/8/6～2010/8/9，1,000,000 円，研究代表者.

E8. 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.

E9. 量子鍵配送方式に関する研究,株式会社 東芝,2012年7月1日～2013年3月31日,1,000,000円，研究代表者.

E10. 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」，2013/3/4～2013/3/7，600,000 円，研究代表者.

E11. 文部科学省，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)，150,000 円，FY2012，運営責任者.

E12. ブラザー工業、エクシング、産総研、音声データの透かし技術

E13. 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.

E14. 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）,2013 年 7 月 1 日～2014 年 3 月 31 日，千葉大学 500,000 円 （全体 1,000,000 円）.千葉大学側研究代表者.

E15. 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，10,700,000 円，研究分担者，FY2014-2016.

E16. 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.

E17. 分散協調型機械学習の研究開発, 三菱電機, 1,000,000 円, 研究代表者, 2015/9/7-2017/3/15.

E18. 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, FY2016-FY2018.

E19. 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, FY2016-FY2018.

特許（取得済）　７件

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

口頭発表

（招待・依頼講演　国際 3 件，招待・依頼講演 国内　１８件，
国際（査読あり）34 件，国際（査読無し）１件，国内（査読なし）６２件）

招待・依頼講演 国際

1)　Error-Correcting Codes and Cryptography，今井 秀樹、萩原 学，非筆頭，HISC2006，奈良県、2006/05/24

2)　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

3)　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

招待・依頼講演 国内

1) 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

2) 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

3) 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

4) 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

5) 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

6) 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

7) 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

8) 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

9) 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

10) 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

11) 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

12) 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.

13) 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.

14) 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.

15) 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

16) 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

17) 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

18) 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

口頭発表　国際（査読あり）

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

2)　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

3)　A Short Random Fingerprinting Code against a Small Number of Pirates，萩原 学、花岡 悟一郎、今井 秀樹, Applied Algebra, Algebraic Algorithms and Error Correcting Codes，Las Vegas (USA)、2006/02/21

4)　Unconditionally Secure Chaffing-and-Winnowing: A Relationship between Encryption and Authentication，花岡 悟一郎、花岡 裕都子（NTT ドコモ）、萩原 学、渡邊 創、今井秀樹（東大/情報セキュリティ研究センター），16th AAECC Symposium，Las Vegas、2006/02/24

5)　On the Correcting Property of a Two-dimensional Error-correcting Code Based on the Lee Metric on Z_(2^m)，坂内 万里、萩原 学、今井 秀樹，ISITA2006，韓国　ソウル、2006/10/30

6)　On Minimal Length of Quasi Cyclic LDPC Codes with Girth Greater Than or Equal to 6，萩原 学、縫田 光司、北川 隆、Marc Fossorier（ハワイ大学）、今井 秀樹，ISITA2006，韓国　ソウル、2006/10/31

7)　Quantum Secure Direct Communication Protocols for Sending a Quantum State，村上ユミコ（NAIST）、中西正樹（NAIST）、萩原 学、山下茂（NAIST）、中島康彦（NAIST），ISITA2006，韓国　ソウル、2006/11/01

8)　A tracing algorithm for short 2-secure probabilistic fingerprinting codes strongly protecting innocent users，縫田 光司、萩原 学、北川 隆、渡邊 創、小川　一人（NHK 放送技術研究所）、藤津　智（NHK 放送技術研究所）、今井 秀樹，3rd IEEE International Workshop on Digital Rights Management (CCNC 2007 Satellite Workshop)，Nevada, USA、2007/01/11

9)　A short random fingerprint code and its tracing algorithm which uses group testing ，北川 隆、萩原 学，2007 Hawaii and SITA Joing Conference on Information Theory，ハワイ、2007/05/30

10)　Optimization of Tardos's Fingerprinting Codes in a Viewpoint of Memory Amount，縫田 光司、萩原 学、渡邊 創、今井 秀樹，Information Hiding 2007 (IH'07)，Saint-Malo, France、2007/06/13

11)　Quantum Quasi-Cyclic LDPC Codes，萩原 学、今井 秀樹，2007 IEEE International Symposium on Information Theory (ISIT2007)，ニース、2007/06/26

12) An Efficient Tracing Algorithm for a 2-Secure and Short Random Fingerprint Code, 藤津智（日本放送協会　放送技術研究所)、萩原 学、今井 秀樹、北川 隆、縫田 光司、小川一人（日本放送協会　放送技術研究所)、渡邊 創, 2007 International Workshop on Information Hiding and Digital Watermarking, IFIPTM 2007, Moncton, New Brunswick, Canada、2007/07/30

13) A Quantum Secure Direct Communication Protocol for Sending A Quantum State and Its Security Analysis, Yumiko Murakami (Mitsubishi Electric Corporation)、Masaki Nakanishi（Nara Institute of Science and Techonology)、萩原 学、Shigeru Yamashita（Nara Institute of Science and Technology)、Yasuhiko Nakashima（Nara Institute of Science and Technology), The 6th WSEAS International Conference on INFORMATION SECURITY and PRIVACY, スペイン、2007/12/14

14) An Improvement of Tardos's Collusion-Secure Fingerprinting Codes with Very Short Lengths, 縫田 光司、藤津　智（NHK 放送技術研究所)、萩原 学、北川 隆、渡邊 創、小川　一人（NHK 放送技術研究所)、今井 秀樹, Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17), Indian Institute of Science, Bangalore, India、2007/12/17

15) A Study on a Key Establishment Scheme with QC LDPC Codes and UH-Protocols, 松永雄斗（中央大学)、萩原 学、今井 秀樹、古原 和邦, ISITA2008, ニュージーランド、2008/12/08

16) A Group Testing Based Deterministic Tracing Algorithm for a Short Random Fingerprint Code, 北川 隆、萩原 学、縫田 光司、渡邊 創、今井 秀樹, 2008 International Symposium on Information Theory and its Applications (ISITA2008), The Langham Hotel, Auckland, New Zealand、2008/12/09

17) Bounds on The Number of Users for Random 2-secure Codes, 萩原 学、吉田隆弘（中央大学)、今井 秀樹, 18th Symposium on Applied algebra, Algebraic algorithms, and Error Correcting Codes, スペイン、2009/06/08

18) LDPC Codes with Fixed Initialization Decoding over Binary Symmetric Channel, 萩原 学、Marc Fossorier (ETIS ENSEA/UCP/CNRS)、今井 秀樹, ISIT 2010, Austin, Texas、2010/06/13.

19) Lattice path enumeration for 321-avoiding permutations with further restrictions, 萩原 学、井沼 学、冨江雅也（つくば大学), 7th International Conference on Lattice Path Combinatorics and Applications, イタリア（シエナ)、2010/07/05

20) Spatially Coupled Quasi-Cyclic Quantum LDPC Codes, 萩原 学、笠井健太（東京工業大学)、今井 秀樹、坂庭好一（東京工業大学), IEEE International Symposium on Information Theory, Saint Petersburg, Russia、2011/08/01

21) LP Decodable Permutation Codes based on Linearly Constrained Permutation

Matrices，和田山 正（名古屋工業大学)、萩原 学，IEEE International Symposium on Information Theory，Saint Petersburg, Russia、2011/08/01

22) Non-Binary Quasi-Cyclic Quantum LDPC Codes，萩原 学、今井 秀樹、笠井健太（東京工業大学)、坂庭好一（東京工業大学)，IEEE International Symposium on Information Theory，Saint Peterburg, Russia、2011/08/01

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

24) Linear Programming Upper Bounds on Permutation Code Sizes From Coherent Configurations Related to the Kendall-Tau Distance Metric, Fabian Lim (MIT)、萩原 学, IEEE ISIT 2012，MIT、2012/07/01

25) LP decodable permutation codes based on linearly constrained permutation matrices, 和田山 正(名古屋工業大学)、萩原 学, American Mathematics Society, Western Sectional Meeting，Hawaii, USA, 2012/03/03

26) Towards Delserte-type upper bounds on permutation code sizes for the Kendall-Tau distance metric，Fabian Lim（MIT)、萩原 学，American Mathematics Society, Western Sectional Meeting，Hawaii, USA， 2012/03/03

27) Linear Programming Upper Bounds on Permutation Codes Sizes From Coherent Configurations Related to the Kendall-Tau Distance Metric, Fabian Lim, Manabu Hagiwara, ISIT 2012, MIT, 2012/07/06

28) On ML-Certificate Linear Constraints for Rank Modulation with Linear Programming Decoding and its Application to Compact Graphs，萩原 学，ISIT 2012，MIT、2012/07/06

29) Comparing Euclidean, Kendall tau Metrics Toward Extending LP Decoding, Justin Kong (Univ. of Hawaii), Manabu Hagiwara, International Symposium on Information Theory and its Application 2012, Hawaii Convention Center, 2012/10.

30) Weight Enumerator Analysis for (2,P)- and (3,P)-SFA LDPC Codes, Manabu Hagiwara, James Nation (Univ. of Hawaii), International Symposium on Information Theory and its Application 2012, Hawaii Convention Center, 2012/10.

31) Performance Analysis for PUF Data Using Fuzzy Extractor, Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura, CUTE 2013, Vietnam, 2013.

32) Cryptographic Key Generation from PUF Data Using Efficient Fuzzy Extractors, Hyunho Kang, Yohei Hori, Toshihiro Katashita, Manabu Hagiwara, Keiichi Iwamura The 16th International Conference on Advanced Communications Technology (ICACT 2014), Pyeongchang, Korea, February 16-19, 2014, pp.23-26, 2014. (Presentation by Kang on Feb. 17th, 2014).

33) Ryosuke Obi, Manabu Hagiwara, and Reynald Affeldt, Formalization of the Variable-Length Source Coding Theorem: Direct Part, ISITA2014, Oct., Melbourne, 2014.
34) Manabu Hagiwara and Takaaki Sasaki, On the Primitive Polynomial as the Characteristic Polynomial of a Symmetric Companion Matrix, ISITA2014, Oct., Melbourne, 2014.

口頭発表　国際（査読なし）

1) Manabu Hagiwara, Shifted Young diagrams and binary I/D error-correcting codes, SIAM DM16, Georgia state, USA, 2016/06/07 (06/06-06/10), 2016.

口頭発表 国内（査読なし）

1)　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

2)　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

3)　Minuscule Heaps Over Simply-Laced, Star-shaped Dynkin Diagrams, 萩原学, Young 図形をめぐる話題と表現論, 京都大学数理解析研究所、2001/11/07

4)　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

5)　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, 京都大学数理解析研究所、2002/11/08

6)　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

7)　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

8)　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

9)　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

10)　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

11)　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

12)　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

13)　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

14)　量子誤り訂正符号の直和によるクリフォード符号の不変特性、2004/05/25

15)　A characterization of the simply-laced FC-finite Coxeter groups, Manabu Hagiwara, Masao ISHIKAWA, Hiroyuki TAGAWA, FPSAC'04, Voncouver、2004/07/01

16)　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

17)　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

18)　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

19)　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

20)　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

21)　Unconditionally Secure Chaffing-and-Winnowing, 花岡 悟一郎、花岡 裕都子（NTT ドコモ)、萩原 学、渡邊 創、今井秀樹（東大/情報セキュリティ研究センター), 第 28 回情報理論とその応用シンポジウム (SITA2005), 沖縄、2005/11/20

22)　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, 情報理論とその応用シンポジウム, 沖縄、2005/11/21

23)　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（東京大学)、萩原 学、松浦幹太（東京大学)、今井 秀樹, 情報理論とその応用シンポジウム, 沖縄、2005/11/21

24)　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

25)　Tardos 符号の検証, 藤津智（日本放送協会　放送技術研究所)、萩原 学、今井 秀樹、北川 隆、縫田 光司、小川一人（日本放送協会　放送技術研究所)、渡邊 創, 第２９回情報理論とその応用シンポジウム, 北海道函館市、2006/11/30

26)　Tardos 符号の解析と追跡アルゴリズムの改良, 藤津智（日本放送協会　放送技術研究所)、萩原 学、今井 秀樹、北川 隆、縫田 光司、小川一人（日本放送協会　放送技術研究所)、渡邊 創, 第 29 回情報理論とその応用シンポジウム (SITA2006), 北海道函館市、2006/11/30

27)　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

28)　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

29)　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（日本放送協会　放送技術研究所)、萩原 学、今井 秀樹、北川 隆、縫田 光司、小川一人（日本放送

協会　放送技術研究所)、渡邊 創，2007 年暗号と情報セキュリティシンポジウム(SCIS2007)，長崎県佐世保市、2007/01/25

30)　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)，長崎県佐世保市、2007/01/25

31)　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

32)　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

33)　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（中央大学)、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，三重県志摩市阿児町賢島、2007/11/27

34)　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（NHK 放送技術研究所)、今井 秀樹，2008 年暗号と情報セキュリティシンポジウム，宮崎県、2008/01/22

35)　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（中央大学)、萩原 学、美添 一樹（中央大学)、古原 和邦、今井 秀樹，SCIS2008，宮崎県、2008/01/22

36)　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

37)　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，、2008/08/10

38)　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

39)　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（中央大学)、萩原 学、今井 秀樹，LDPC 符号ワークショップ，沖縄県、2008/09/11

40)　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

41)　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，滋賀県大津市、2009/01/20

42)　LDPC 符号を用いた McEliece 署名方式，山川 茂紀（中央大学理工学部)、Cui Yang、萩原 学、古原 和邦、今井 秀樹，ISEC（情報セキュリティ研究会)，函館、2009/03/10

43)　情報部の誤り率が小さい LDPC 符号の構成と解析，松永雄斗（中央大学)、萩原 学、今井 秀樹，ＳＩＴＡ２００９，山口県、2009/12/02

44)　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（中央大学)、萩原 学、今井 秀樹，ＳＩＴＡ２００９，山口県、2009/12/02

45)　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

46)　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，サンポートホール高松、2010/01/20

47)　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（中央大学)、吉田 隆弘、萩原 学、古原 和邦、今井 秀樹，ＳＣＩＳ２０１０，サンポート高松、2010/01/21

48)　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（東京理科大学)、萩原 学、岩村 恵市，ＳＣＩＳ２０１０，サンポート高松、2010/01/21

49)　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

50)　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（中央大学)、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

51)　Quantum Error Correction with Non-Binary LDPC Codes，笠井健太（東京工業大学)、萩原 学、今井 秀樹、坂庭好一（東京工業大学)，IBIS 2010，東京大学、2010/11/04

52)　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，小栁裕嵩（中央大学)、萩原 学、今井 秀樹，SITA2010，長野県、2010/12/02

53)　Quantum Error Correction with Non-Binary LDPC codes，笠井健太（東京工業大学)、萩原 学、今井 秀樹、坂庭好一（東京工業大学)，SITA2010，長野、2010/12/02

54)　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（京都大学)、田中利幸（京都大学)、今井 秀樹，SITA2010，長野、2010/12/02

55)　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.

56)　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.

57)　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.

58) 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.

59) On formalization of basic geometric topology, Ken'ichi Kuga, Manabu Hagiwara, TPP (Theorem proving and provers for reliable theory and implementations) 2014, 九州大学, 2014/12/05.

60) 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，富山県宇奈月ニューオータニホテル，2014/12/11.

61) 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.

62) 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

受賞

1) 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.