様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２５ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５４０１１１

研究課題名（和文）組合せ論的マルチメディア指紋符号とその不正者追跡アルゴリズムの研究

研究課題名（英文）Combinatorial multimedia fingerprinting codes and their corresponding colluder-tracing algorithms

研究代表者

繆　いん（Miao, Ying）

筑波大学・システム情報系・教授

研究者番号：１０３０２３８２

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：　デジタルコンテンツの不正な流通を防ぐために，不正ユーザの結託攻撃に耐性を持つ指紋符号を構成し，それに基づいた不正ユーザ追跡するアルゴリズムを開発した．（１）指紋符号の一種である分離可能符号の符号語数の上界を改善し，上界に達する最適な分離可能符号の無限系列を射影平面などを用いて構成した．（２）効率の高い追跡アルゴリズムを開発するために，強分離可能符号を導入し，差行列を用いて無限系列を構成した．（３）有限幾何に基づいて，完全ハッシュ関数族の無限系列も構成した．
　デジタル指紋の基礎理論の一つである組合せ論やデジタル指紋と密接な関係を持つ遺伝子解析や情報通信についても研究がなされた．

研究成果の概要（英文）：To prevent the unauthorized redistribution of digital contents, we have constructed several kinds of fingerprinting codes which can resist the collusion attacks mounted by malicious authorized users, and developed colluder-tracing algorithms based on such codes. We have improved the upper bound on the size of a separable code, and then by using projective planes, we have constructed several infinite series of optimal separable codes in which the sizes attain the improved upper bound. To improve the efficiency of the tracing algorithm based on separable codes, we have introduced strongly separable codes, and constructed several infinite series of strongly separable codes by means of difference matrices. We have also constructed several infinite series of perfect hash families from finite geometry.
　By using the ideas obtained in the investigation of digital fingerprinting, we have also studied the related combinatorics, bioinformatics and information communication.

研究分野：組合せ論

キーワード：デジタル指紋　組合せ論　指紋符号　追跡アルゴリズム　分離可能符号　完全ハッシュ関数族　情報通信　遺伝子解析

## １．研究開始当初の背景

デジタル指紋とは，個々のコンテンツにユーザを特定する指紋と呼ばれる情報を利用者に分からないように埋込んでおき，コンテンツが不正に流通した際に，埋込まれた指紋から不正を行ったユーザを追跡する技術である．

複数の不正なユーザがそれぞれの配布コンテンツを比較して埋込まれた指紋を改ざんする結託攻撃が行われると，もともと埋込まれた指紋が改ざんされてしまうため，不正者を特定できなくなるだけでなく，正当なユーザが告発される恐れもある．平均化攻撃は，マルチメディアのデジタル指紋への有効な結託攻撃の一つとして広く知られている．

Boneh・Shawはデジタルコンテンツへの結託攻撃問題を解決するために，1998年にデジタル指紋を導入し，結託攻撃に対して耐性をもつframeproof符号などの指紋符号を提案した．Barg他（2003）は代数幾何符号及びリスト復号アルゴリズムを用いて，効率の高い不正者追跡アルゴリズムを開発した．Tardos（2008）は確率的指紋符号により，デジタル指紋に関する研究を行った．またTrappe他（2003）は信号空間がヒルベルト空間の部分空間であることを利用し，マルチメディアコンテンツや指紋をベクトルと見なし，指紋の成分ごとのAND演算を用いて，平均化攻撃に対して耐性を持つAND-結託耐性符号を提案し，デジタル指紋のマルチメディアコンテンツ著作権保護への応用の扉を開いた．

残念ながら，従来の指紋符号では，結託攻撃による不正者の見逃しやえん罪を防ぐために，符号長を極めて長くする必要があった．

Cheng・繆（2011）はデジタル指紋とグループ検査との関連を明らかにし，デジタル指紋の本質的問題とは，ユーザの集合からどんな部分集合の族を選ぶか，という組合せ論的問題であることを確認した．Cheng・繆（2011）では指紋の成分ごとのOR演算も用いて，平均化攻撃に対して耐性を持つ論理結託耐性符号を提案し，符号長の短縮などにより，Trappe 他（2003）の不正者追跡アルゴリズムを見直し，効率を大幅に改善した．論理結託耐性符号を構成するために，分離可能符号の概念も提案した．

## ２．研究の目的

本研究では，デジタルコンテンツ（特にマルチメディアコンテンツ）の不正な流通を防ぐためのデジタル指紋理論の数理的研究を行う．デジタル指紋理論では，ユーザを特定する指紋をコンテンツに埋込んで，海賊版で検知された情報から，不正な指紋を作り出し，その海賊版を作った不正ユーザを追跡する．我々は，組合せ理論や符号理論などを用いて，不正者の結託攻撃に耐性を持つ指紋符号を構成し，不正者を効率よく追跡するアルゴリズムの開発を行う．

## ３．研究の方法

Cheng・繆（2011）が発見したグループ検査とマルチメディア指紋の間の緊密な関係により，デジタル指紋理論（特にマルチメディア指紋）に関する新しい研究方向性を示した．本研究では，各種のグループ検査手法を検討しながら，新しいマルチメディア指紋を組合せ論的立場から研究する．

## ４．研究成果

デジタルコンテンツの不正な流通を防ぐために，不正ユーザの結託攻撃に耐性を持つ指紋符号を構成し，それに基づいた不正ユーザを追跡するアルゴリズムを開発した．

分離可能符号は指紋符号の一種であり，それに基づいた追跡アルゴリズムは，ユーザ数 $M$ が分離可能符号の符号語数の最大値を超えない場合，かつ不正ユーザ数がある定められた定数 $t$ を超えない場合では，不正ユーザ全員を捕まえることができる．

Cheng・Ji・繆（[11]）は，分離可能符号の符号語数の上界の導出や最適な分離可能符号の構成を行った．Cheng・Fu・Jiang・Lo・繆（[4]）は，その上界を更に改善し，新しい上界に達する最適な分離可能符号の無限系列を射影平面を用いて構成した．

分離可能符号に基づいた追跡アルゴリズムの計算量は $O(M^t)$ であり，非効率的である．効率の高い追跡アルゴリズムを開発するために，Jiang・Cheng・繆（[1]）は強分離可能符号を導入し，それに基づいた追跡アルゴリズムの計算量は $O(M)$ であることを示した．組合せ的アプローチにより，強分離可能符号の無限系列も構成した．

完全ハッシュ関数族はデジタル指紋だけでなく，ほかの情報分野でもよく使われている．藤原（[2]）は有限幾何に基づいて，完全ハッシュ関数族の無限系列を構成した．

指紋符号及び不正ユーザ追跡アルゴリズムは，遺伝子解析などに用いられるモチーフ発見問題やグループ検査理論と密接な関係がある．デジタル指紋の研究で得られた知見を遺伝子解析へ適用し，繆や神保は面白い結果を得た（[7]，[8]，[13]）．

その知見の情報通信への適用も広範囲にわたった（[3]，[6]，[9]，[10]）．

藤原と神保は基礎理論である組合せ論についても研究し，各種の組合せデザインを構成した（[5]，[12]，[14]）．

我々の論文が，既に一流の国際学術誌 IEEE Transactions on Information Theory などに掲載された．組合せ的アホローチからデジタル指紋や関連分野に関する研究か急速に進む中で，我々の研究結果は大きく貢献した．

## ５．主な発表論文等

〔雑誌論文〕（計 14 件）

[1] J. Jiang, M. Cheng and Y. Miao, Strongly separable codes, Designs, Codes and Cryptography, **査読有**, to appear, 2015.
DOI: 10.1007/s10623-015-0050-1

[2] R. Fuji-Hara, Perfect hash families of strength three with three rows from varieties on finite projective geometries, Designs, Codes and Cryptography, **査読有**, to appear, 2015.
DOI: 10.1007/s10623-0052-z

[3] Y. Lin, M. Mishima and M. Jimbo, Optimal equi-difference conflict-avoiding codes of weight four, Designs, Codes and Cryptography, **査読有,** to appear, 2015.
DOI: 10.1007/s10623-014-0030-x.

[4] M. Cheng, H.-L. Fu, J. Jiang, Y.-H. Lo and Y. Miao, New bounds on 2-separable codes of length 2, Designs, Codes and Cryptography, **査読有**, Vol. 74, 2015, 31-40.
DOI: 10.1007/s10623-013-9849-9

[5] M. Hirao, M. Sawa and M. Jimbo, Constructions of Φ p-optimal rotational designs on the ball, Sankhya -- The Indian Journal of Statistics, **査読有**, Vol. 77, 2015, 211-236.
DOI: 10.1007/s13171-014-0053-4

[6] J. Chen, D. Wu and Y. Miao, Bounds and constructions for (v,W,2,Q)-OOCs, Discrete Mathematics, **査読有**, Vol. 328, 2014, 16-22.
DOI: 10.1016/j.disc.2014.03.028

[7] X. Wang and Y. Miao, GAEM: A hybrid algorithm incorporating GA with EM for planted edited motif finding problem, Current Bioinformatics, **査読有**, Vol. 9, 2014, 463-469.
DOI: 10.2174/1574893609666140901222327

[8] X. Wang, Y. Miao and M. Cheng, Finding motifs in DNA sequences using low-dispersion sequences, Journal of Computational Biology, **査読有**, Vol. 21, 2014, 320-329.
DOI: 10.1089/cmb.2013.0054

[9] Y. Lin and M. Jimbo, Extremal properties of t-SEEDs and recursive constructions, Designs, Codes and Cryptography, **査読有**, Vol. 73, 2014, 805-823.
DOI: 10.1007/s10623-013-9829-0

[10] Y. Lin, M. Mishima, J. Satoh and M. Jimbo, Optimal equi-difference conflict-avoiding codes of odd length and weight three, Finite Fields and Their Applications, **査読有**, Vol. 26, 2014, 49-68.
DOI: 10.1016/j.ffa.2013.11.001

[11] M. Cheng, L. Ji and Y. Miao, Separable codes, IEEE Transactions on Information Theory, **査読有**, Vol. 58, 2012, 1791-1803**.**
DOI: 10.1109/TIT.2011.2174614

[12] D. Wu, R. Fuji-Hara, D. Li and S. Chen, The existence of doubly disjoint (my+1,m, m,m-1) difference families, Ars Combinatoria, **査読有**, Vol. 104, 2012, 197-209**.**
http://www.combinatorialmath.ca/arscombinatoria/

[13] T. Kanamori, H. Uehara and M. Jimbo, Pooling design and bias correction in DNA library screening, Journal of Statistical Theory and Practice, **査読有**, Vol. 6, 2012, 220-238.
DOI: 10.1080/15598608.2012.647585

[14] K. Momihara, M. Mishima and M. Jimbo, A decomposition of the 2-design formed by the planes in AG(2n,3), Finite Fields and Their Applications, **査読有**, Vol. 18, 2012, 956-970**.**
DOI: 10.1016/j.ffa.2012.04.001

〔学会発表〕（計 15 件）

[1] Y. Miao, Strongly separable codes, ALCOMA 15, Algebraic Combinatorics and Applications, Conference in Memory of Alex Kohnert, March 15-20, 2015, Kloster Banz, Germany.

[2] M. Jimbo, Cyclic codes with large minimum distances and related combinatorial designs, ALCOMA 15, Algebraic Combinatorics and Applications, Conference in Memory of Alex Kohnert, March 15-20, 2015, Kloster Banz, Germany.

[3] Y. Miao, On an extension of collaboration distance, **研究集会「実験計画法およびその周辺の組合せ構造」, 2014 年 12 月 13 日-15 日, 城崎国際アートセンター（兵庫県）.**

[4] R. Fuji-Hara, Classification of Authentication codes and a new model, **研究集会「実験計画法およびその周辺の組合せ構造」, 2014 年 12 月 13 日-15 日, 城崎国際アートセンター（兵庫県）.**

[5] Y. Miao, Fingerprinting codes and

related extremal bipartite graphs, Japan Conference on Graph Theory and Combinatorics, May 17-21, 2014, Nihon University, Tokyo.

[6] Y. Miao, Beyond separable codes, The 3rd Taiwan-Japan Conference of Combinatorics and its Applications, March 21-23, 2014, National Chiayi University, Taiwan. **招待講演.**

[7] R. Fuji-Hara, Descendent vectors and frameproof codes of binary case, The 3rd Taiwan-Japan Conference of Combinatorics and its Applications, March 21-23, 2014, National Chiayi University, Taiwan. **招待講演.**

[8] M. Jimbo, Generalized 1-factorizations over C and quasi-difference matrices, The 3rd Taiwan-Japan Conference of Combinatorics and its Applications, March 21-23, 2014, National Chiayi University, Taiwan. **招待講演.**

[9] R. Fuji-Hara, The unification of combinatorial designs with multi-structures, International Conference on Interdisciplinary Mathematics 2013, November 10-12, 2013, Kitakyusyu International University Conference Center, Fukuoka. **招待講演.**

[10] R. Fuji-Hara, Descendent sets and codes, **平成 25 年度 RIMS 共同研究「デザイン、符号、グラフ及びその周辺」, 2013 年 7 月 1 日-3 日, 京都大学数理解析研究所 (京都府). 招待講演.**

[11] Y. Miao, Expanded separable codes, The 11th International Conference on Finite Fields and Their Applications, June 22-26, 2013, Otto-von-Guericke University, Ger- many.

[12] R. Fuji-Hara, Descendent sets and codes, The 11th International Conference on Finite Fields and Their Applications, June 22-26, 2013, Otto-von-Guericke University, Germany.

[13] Y. Miao, Digital fingerprinting and related topics, 2012 International Workshop on Discrete Mathematics, December 8-10, 2012, Fuzhou University, China.

[14] Y. Miao, Anti-collusion properties of fingerprinting codes, The 2nd Japan-Taiwan Conference of Combinatorics and its Applications, November 10-12, 2012, Nagoya University, Nagoya.

[15] R. Fuji-Hara, Descendent sets and codes, The 2nd Japan-Taiwan Conference of Combinatorics and its Applications, November 10-12, 2012, Nagoya University, Nagoya.

## ６．研究組織

(1)研究代表者

繆 いん（MIAO, Ying）
筑波大学・システム情報系・教授
研究者番号：10302382

(2)研究分担者

藤原 良叔（FUJIWARA, Ryoshuku）
筑波大学・システム情報系・教授
研究者番号：30165443

(3)連携研究者

神保 雅一（JIMBO, Masakazu）
名古屋大学・情報科学研究科・教授
研究者番号：50103049