氏　名（本籍）	蒋　静
学 位 の 種 類	博　士（工学）
学 位 記 番 号	博　甲　第　　7271　　号
学位授与年月日	平成　27　年　3　月　25　日
学位授与の要件	学位規則第４条第１項該当
審 査 研 究 科	システム情報工学研究科
学位論文題目	On Codes for Multimedia Fingerprinting: Traceability, Bounds, and Constructions （マルチメディアのための指紋符号：追跡生，バウンド，そして構成法）

主　　査	筑波大学	教授	Ph.D. in Combinatorics and Optimization	藤原　良叔
副　　査	筑波大学	准教授	博士（学術）	八森　正泰
副　　査	筑波大学	教授	工学博士	岸本　一男
副　　査	筑波大学	助教	博士（情報理工学）	安藤　弘泰
副　　査	筑波大学	教授	博士（理学）	繆　瑩
副　　査	筑波大学	准教授	博士（工学）	古賀　弘樹
副　　査	神戸大学	准教授	博士（情報科学）	澤　正憲

論　文　の　要　旨

本論文のテーマは、マルチメディア・コンテンツの違法コピーの配布を抑止するため、線形結託攻撃に対処できる新たなアンチ結託符号と、それを用いた結託者の追跡アルゴリズムの開発である。

第１章でマルチメディア・コンテンツの違法コピーの配布が近年問題になっていることを指摘し、マルチメディア指紋のこれまでの研究成果を概観している。結託した t 人の利用者が彼らのマルチメディア指紋から新たな指紋を線形結合で合成することによって身元を隠す線形結託攻撃を紹介し、この種の攻撃に対して結託者を追跡するための既存のアンチ結託符号を紹介している。

第２章では、既存の LACC（logical anti-collusion code）とそれに基づいた結託者追跡アルゴリズムを紹介し、SC（separable code）を用いて LACC を構成する既知の方法を説明している。マルチメディア指紋において、SC の構成とその利用可能者人数 M_{SC}の上界値の計算は重要な課題である。この章の前半では、符号の長さ２の SC について、M_{SC}の上界値計算問題を内周（girth）が６の二部グラフの最大枝数計算問題に変換し、これによって M_{SC}の上界値に関する既存結果を改善した。さらに、射影平面を用いて、M_{SC}の新しい上界値に達成する最適な SC の無限系列を数多く構成した。第２章の後半では、長さ４の SC を不完全方陣によって特徴づけており、これによって M_{SC}の上界値に漸近的に達成する漸近的

最適な SC の無限系列を数多く構成した。

第３章では、LACC に基づいた結託者追跡アルゴリズムの計算量は、アンチ結託符号の長さ n や利用可能者人数 M、結託者人数 t に依存し $O(nM^t)$ であるため、これを改善するために、SSC（strong separable code）を導入し、２値の SSC を用いた計算量が $O(nM)$ である追跡アルゴリズムを提案している。既知の q 値 SSC より新しい SSC を構成する連結方法を述べた後、SSC と SC や FPC（frameproof code）など既知のアンチ結託符号の関係を示し、長さ２においては SSC は SC と同値であることを指摘した。さらに、長さ３では SSC を構成するために、SSC の禁止構造（forbidden configuration）を洗い出し、これによって任意の自然数 q に対して q 値 SSC を構成した。構成された長さ３の q 値においての SSC は FPC に比べ利用可能者人数は約１５％増えた。

第４章では、結託者人数が高々 t である場合、SC や SSC を用いた追跡アルゴリズムを適用することにより、結託者全員が発見できるが、しかしながら、SC や SSC の利用可能者人数が多くない。この弱点を克服するために、MIPPC（multimedia identifiable parent property code）を導入し、２値 MIPPC に基づいた結託者追跡アルゴリズムを提案した。MIPPC の利用可能者人数は SC や SSC、FPC の利用可能者人数より多いし、MIPPC に基づいた追跡アルゴリズムを適用することにより、少なくとも１人の結託者を発見できることを述べている。既知の q 値 MIPPC より新しい MIPPC を構成する連結方法を示した後、MIPPC の利用可能者人数 M_{MIPPC} の上界値を調べ、内周（girth）が８の二部グラフの最大枝数計算問題に帰着させた。射影平面を用いて、M_{MIPPC} の上界値に達成する最適な MIPPC の無限系列を数多く構成した。

第５章では、計算量が $O(nM^t)$ である MIPPC に基づいた追跡アルゴリズムを改善するために、SMIPPC（strong multimedia identifiable parent property code）を導入し、２値 SMIPPC に基づいた計算量が $O(nM)$ である結託者追跡アルゴリズムを提案した。 既知の q 値 SMIPPC より新しい SMIPPC を構成する連結方法を述べた後、長さ２の SMIPPC は長さ２の MIPPC と同値であることを指摘した。さらに、長さ３の SSC を構成するために、長さ３の SMIPPC の禁止構造を洗い出し、巡回的差行列（cyclic difference matrix)を用いて、任意の自然数 $q \equiv 0,1,2,5 \pmod 6$ に対して長さ３の最適な q 値 MIPPC を構成した。

第６章において、本研究の結果全般に対する考察と今後の研究課題の展望が示されている。

審　査　の　要　旨

【批評】

既存の SC (separable codes) の改善を行うとともに、それを拡張し、すべての結託者を発見可能な SSC (strong separable code) を提案した。そして追跡アルゴリズムの計算量を SC の $O(nM^t)$ から $O(nM)$ に改善した。つぎに利用者の数を増やすために、MIPPC (multimedia identifiable parent property code) およびその２値の場合の追跡アルゴリズム、 $O(nM^t)$、 を提案した。そしてグラフ理論上の問題に帰着させ上界値に達する最適な MIPPC の無限系列を多く構成した。最後に MIPPC の計算量を改善するために S(strong)MIPPC を提案し、2 値の場合、追跡アルゴリズムを計算量が $O(nM)$ となるように改善した。また長さ３の SMIPPC を組合せ理論の結果を使って任意の自然数 $q \equiv 0,1,2,5 \pmod 6$ に対して最適な q 値 MIPPC を構成した。 これらの研究成果はこの分野に大きく貢献しており、博士論文としての水準に達している。

【最終試験の結果】

平成 27 年２月９日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。その結果、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。