

氏名(本籍)	范金萍(中華人民共和国)		
学位の種類	博士(社会工学)		
学位記番号	博甲第 9683 号		
学位授与年月日	令和 2 年 9 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	Signature Coding Schemes for Multiple Access Channels with Applications to Multimedia Fingerprinting and Group Testing (多重接続チャンネルのための署名符号化スキーム及びそのマルチメディア指紋やグループ検査への応用)		
主査	筑波大学 教授	博士(理学)	繆 瑩
副査	筑波大学 教授	博士(理学)	繁野 麻衣子
副査	筑波大学 教授	博士(工学)	張 勇兵
副査	筑波大学 准教授	博士(学術)	八森 正泰
副査	筑波大学 准教授	博士(理学)	佐野 良夫

論文の要旨

本論文は、多重接続通信における、受信側がアクティブユーザを識別できる署名符号方式及びそのマルチメディア指紋理論やグループ検査理論への応用に関して高性能なスキームを構成することを目的としている。第 1 章では、アクティブユーザを識別するために、一意復号可能符号を利用する必要があることを指摘し、weighted binary adder channel (WbAC) とそのマルチメディア指紋への応用、及び OR (論理和) チャンネルとそのグループ検査への応用のこれまでの研究結果を概観している。第 2 章で研究を進めるための、集合論やグラフ理論などの予備知識を提供している。第 3 章では、無雑音 WbAC と OR チャンネルで使われる幾つかの一意復号可能符号やその性質を表現する行列を紹介した後、第 4 章でその重要な一つである WbAC 署名符号に着目している。WbAC 署名符号と二部グラフの間の興味深い関係を明らかにし、更に極値グラフ理論により、WbAC 署名符号のユーザ数に関する上界を与えている。そして高性能な署名符号の構成法を 2 件提案している。また、幾何学的な観点から、有雑音 WbAC に対して一意復号可能符号の存在性を否定し、有雑音 WbAC のための符号を導入している。第 5 章で分離可能符号について、極値集合論や確率論的手法により、ユーザ数の上下界を与え、従来の上下界を大幅に改善している。第 6 章では、OR チャンネルにおける分離可能行列と隔離行列に基づく一意復号可能スキームの復号効率やユーザ数を改善するため、強分離可能行列の概念を導入した。それに基づく復号アルゴリズムの高効率性を示した上で、確率論的手法により、強分離可能行列のユーザ数に関する良い下界を与えた。第 7 章では、本研究の結果全般に対する要約や今後の研究課題の展望が示されている。

審査の要旨

【批評】

本論文は、数年前まで各々が独自に発展してきたマルチメディア指紋理論とグループ検査理論を多重接続通信の観点で体系化することを目的としており、挑戦的な研究である。情報の電子化は利便性を向上する一方で、複製や改竄など攻撃を容易にし、電子データの著作権保護が必要不可欠である。Boneh *et al.* (IEEE Trans. Inf. Theory, 1998) や Liu *et al.* (Hindawi, 2005) などは電子データの著作権を保護できる指紋符号を提案した。また、多くの検体の集合からある特徴を持つ極めて稀な少数の検体を効率よく識別するため、Dorfman (Ann. Math. Stat., 1943) はグループ検査を導入し、検査行列を調べた。最近の研究により、マルチメディア指紋やグループ検査は多重接続通信に緊密な関係があることが少しずつ明らかになっている。本論文では、指紋符号や検査行列を多重接続通信の署名符号として捉え、極値グラフ理論や極値集合論、確率的な手法などを駆使し、様々な署名符号を調べ、ユーザ数の新しい上下界を計算する上で、より多いユーザ数を持つ復号効率の高い署名符号を構成した。これらの研究成果はこの分野の発展に大きな貢献を果たしていると言える。

しかしながら、本論文には以下のような課題が残されている。まず、本論文で示された WbAC 署名符号のユーザ数に関する上界はタイトであるか不明である。この原因で、署名符号の良さを評価し難い。WbAC 署名符号のユーザ数に関する上下界の間のギャップを埋めるために、新しい技術の開発につながる可能性が高く、研究を進める価値が大いにある。また、本論文で導入された強分離可能行列の最大列数は分離可能行列の最大列数とほぼ同じであるかどうかは不明である。もしほぼ同じでないならば、新しい検査行列の概念を提案する価値も大いにある。

以上のような課題が残されているものの、本論文が行なった三分野（多重接続通信、マルチメディア指紋、グループ検査）に共通する数学的構造の性質や構成法を統一的に扱い、その数学的構造に関する理論体系の構築に関する試みが、今後の発展の土台となる研究として高く評価できる。そのため、本論文を博士（社会工学）に相応しい内容だと判断する。

【最終試験の結果】

令和2年7月28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（社会工学）の学位を受けるに十分な資格を有するものと認める。