氏　名（本籍）	邵 敏锋（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　9684　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	Algebraic Manipulation Detection Codes and Related Structures （代数改竄検出符号および関連構造）

主　査	筑波大学　教授	博士（理学）	繆　瑩
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（情報理工学）	安東 弘泰
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	博士（工学）	古賀　弘樹

論　文　の　要　旨

本論文は、プライベートストレージデバイス（private storage device）に置いている秘密データに対する代数的改竄（algebraic manipulation）攻撃を防ぐための代数改竄検出符号（algebraic manipulation detection code，AMD 符号）およびその関連構造の性質や構成法に関する研究である。

第１章では、AMD 符号の概念を説明した後、その秘密分散法（secret sharing scheme）やファジー抽出器（fuzzy extractor）への応用を紹介し、AMD 符号のこれまでの研究結果を概観している。

第２章では研究を進めるために組合せ論や情報理論などの予備知識を提供している。

第３章では、AMD 符号の構成に重要な役割を果たしていた様々な既存の外部差集合族（external difference family）を紹介した後、有界標準加重外部差集合族（bounded standard weighted external difference family，BSWEDF）の概念を新たに導入し、BSWEDF の性質を調べ、有限群や有限体などに基づき BSWEDF を構成している。

第４章では、弱 AMD 符号と外部差集合族との緊密な関係を明らかにし、BSWEDF により、弱 AMD 符号の組合せ的特徴付を与え、弱 AMD 符号を構成している。高非線形関数（highly nonlinear function）により、組織的（systematic）弱 AMD 符号も構成している。

第５章で組織的強 AMD 符号と高非線形関数との関係を調べ、高非線形関数により組織的強 AMD 符号を構成している。また逆に組織的 AMD 符号により高非線形関数も構成している。強 AMD 符号に関する組合せ的構成法も提案している。

第６章では、本研究成果全般の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】

近年、情報の電子化は利便性を向上する一方で、盗聴や改竄など攻撃行為を容易にし、機密データの保護が必要不可欠になっている。Cramer *et al.*（Eurocrypt 2008）は秘密データに対する攻撃の一種である代数的改竄攻撃を防ぐための代数改竄検出符号（AMD 符号）を提案した。本論文は、組合せデザイン理論や高非線形関数理論に基づいて AMD 符号及びそれらの構造の性質や構成法に関する研究である。先行研究により、一部の AMD 符号と外部差集合族や高非線形関数との関係が明らかされたが、AMD 符号と外部差集合族や高非線形関数との関係の全体像の解明が不十分であった。本論文は、AMD 符号の性質を詳しく調べ、それに対応する組合せ的構造、すなわち、有界標準加重外部差集合族（BSWEDF）、及び関数の部分非線形性（partial nonlineality）という新しい概念を導入することで、AMD 符号に関する研究の方向性を明示している。また、代数的・組合せ的手法を用いて、BSWEDF 及び高非線形関数を利用し、効率的な AMD 符号の無限系列を幾つか構成した。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、本論文は以下のような課題が残されている。まず、BSWEDF が AMD 符号の構成に極めて重要であることが示されたが、BSWEDF における理論的体系の構築が行われたとは言い難い。Wilson の差集合族理論を参照しながらの、BSWEDF に関する体系的な研究を期待する。次に、組織的 AMD 符号は関数の非線形性ではなく、関数の部分非線形性に関わっていることが本論文で明確に指摘されたが、関数の部分非線形性における研究は、残念ながら十分とは言えない。組織的 AMD 符号は情報システムの信頼性と安全性の向上に関わっているので、部分非線形性の高い関数を探し、最適な組織的 AMD 符号の構成を期待する。

以上のような課題が残されているものの、本論文で行なった研究は今後の機密データ保護技術を発展する土台となる可能性が高く、多分野（暗号理論、符号理論、組合せ論）融合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。