New Progress on Combinatorial Schemes for Broadcast Encryption and Codes for Multimedia Fingerprinting

著者	GU YUJIE
発行年	2018
その他のタイトル	放送型暗号の組合せ的構造及びマルチメディア指紋符号に関する進展
学位授与大学	筑波大学 (University of Tsukuba)
学位授与年度	2017
報告番号	12102甲第8506号
URL	http://hdl.handle.net/2241/00152827

氏　名	GU YUJIE
学位の種類	博　士（社会工学）
学位記番号	博　甲　第　８５０６　号
学位授与年月日	平成　３０年　３月　２３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	New Progress on Combinatorial Schemes for Broadcast Encryption and Codes for Multimedia Fingerprinting （放送型暗号の組合せ的構造及びマルチメディア指紋符号に関する進展）

主　査	筑波大学　教授	博士（理学）	繁野 麻衣子
副　査	筑波大学　准教授	博士（情報理工学）	小林 佑輔
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（情報理工学）	安東 弘泰
副　査	神戸大学　准教授	博士（情報科学）	澤　正憲
副　査	筑波大学　教授	博士（理学）	繆　瑩

論　文　の　要　旨

電子データの著作権保護は、現代社会における重要な挑戦的課題の一つであると同時に、その解決は組合せ数学の発展に寄与している。本論文のテーマは、放送型暗号の復号化鍵や電子データの不法な再配布を抑止するため、結託攻撃に対処できる組合せ的スキームや指紋符号の性質及び構成法に関する研究であり、組合せ数学のなかの極値集合論、極値グラフ理論、確率論的手法、組合せデザイン理論を駆使している。

第１章で電子データ著作権侵害が近年問題になっていることを指摘し、結託攻撃に対処できる組合せ的スキームや指紋符号のこれまでの研究成果を概観している。結託攻撃とは、複数の利用者が結託し、彼らの復号化鍵や電子指紋を重ね合わせることによって身元を隠す攻撃である。第２章で研究を進めるための組合せ数学における予備知識を提供している。

第３章で放送型暗号の復号化鍵の不法な再配布を抑止できる幾つかの組合せ的スキームを紹介した後、第４章でその重要な一つである追跡可能スキーム（traceability scheme）に焦点を絞っている。追跡可能スキームとCFF（cover-free family）の間の興味深い関係を明らかにする上で、極値集合論により、追跡可能スキームの利用可能者人数に関するタイトな上界を与え、従来の上界を大幅に改善している。組合せデザイン理論を用い、利用可能者人数が最大になる追跡可能スキームも構成している。

第５章では、親識別（parent-identifying）概念を統一し、親識別スキームを提案している。親識別スキームの利用可能者人数計算問題をTuran型問題として捉え、極値集合論や極値グラフ理論を用

いて、その上界を大幅に改善している。さらに、確率論的手法により、その下界も導出している。

第６章では、CFF に基づくスキームの結託耐性を改善するために、UIBF（union-intersection bounded family）の概念を導入し、極値集合論や確率論的手法により、UIBF の利用可能者人数に関する上下界を与えている。

第７章は MIPPC（multimedia parent-identifying code）の利用可能者人数の下界値の計算がテーマである。MIPPC の禁止構造を示す上で、確率論的手法により、MIPPC の利用可能者人数の下界値を与えている。

第８章において、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】

現代社会において、情報の電子化は利便性を向上する一方で、盗聴・複製・改ざんなどを容易にし、電子データの著作権保護や暗号化することが必要不可欠である。Boneh *et al.*（IEEE Trans. Inf. Theory, 1998）や Hollmann *et al.*（J. Combin. Theory Ser. A, 1998）は電子データの著作権を保護できる指紋符号を提案し、Chor *et al.*（Crypto’94, 1994; IEEE Trans. Inf. Theory, 2000）や Stinson *et al.*（SIAM J. Discrete Math., 1998）は不正者追跡できる放送型暗号を提案した。

本研究は組合せ数学を駆使し、放送型暗号の復号化鍵や電子データの不正な再配布を抑止するための不正者追跡機能を持つ放送型暗号や指紋符号を調べ、長年未解決であった利用可能者人数のタイトな上界と新しい下界を計算し、利用可能者人数が最大になる不正者追跡機能を持つ放送型暗号を世界で初めて構成した。特に上界の導出方法は放送型暗号の分野のみならず、組合せ数学分野でも高く評価される成果であり、国際学術雑誌にも掲載されている。

以上より、これらの研究成果はこの分野に大きく貢献し、博士論文としての高い水準に達していると判断する。

【最終試験の結果】

平成３０年２月８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。