

2023年度共同利用研究報告書

2024年03月05日

所属・職名 熊本大学 半導体・デジタル研究教育機構 総合情報学部門・准教授
佐竹 翔平

		整理番号	2023a017	
1.研究計画題目	エクspanderグラフの新しい構成手法の確立とその応用2			
2.新規・継続	継続			
3.種別	若手・学生研究			
4.種目	短期共同研究			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	佐竹 翔平		
	所属 部局名	熊本大学 半導体・デジタル研究教 育機構 総合情報学部門	職 名	准教授
7.研究実施期間	2023年09月04日(月曜日)～2023年09月08日(金曜日)			
8.キーワード	エクspanderグラフ, 組合せ論・組合せ最適化, 群論, 整数論, 耐量 子計算機暗号, 符号理論, 理論計算機科学, 学習理論			
9.参加者人数	97人			

10.本研究で得られた成果の概要

本共同研究の目的として以下の2点を挙げていた.

- 代数的な構成と組合せ論・アルゴリズム的な構成をハイブリッドさせ, 両者の利点を抽出した新しい構成手法を編み出す.
- エクspanderの暗号理論, 符号理論, 学習理論などの情報科学への応用にも目を向け, 構成したエクspanderの応用を検討する.

本共同研究によって, 目的(i), (ii)に関する昨年度からの共同研究が順調に進展してきており, その成果も査読付き論文や報告集論文にて発表されている. また, 数学と情報科学のインタラクションに位置する共同研究として, 暗号学的ハッシュ関数や誤り訂正符号の数理的設計などの新たな共同研究プロジェクトも本共同利用研究を起点にスタートしており, 定期的な研究議論を継続中である. さらに, 企業側研究者との議論を通して, 暗号理論などへの応用・実装に関する議論も大きく進展しており, 引き続き定期的な議論と成果発表を行っていく予定である.

報告書は 2026 年 4 月に公開予定

開催日：2023/09/04~2023/09/08

エクパンダーグラフの新しい構成手法の確立とその応用2 | 共2023a017

カテゴリー：イベント

タグ：

若手研究

短期共同研究

開催概要

- 開催方法：九州大学 伊都キャンパスとZoomミーティングによるハイブリッド開催
- 開催場所：九州大学 伊都キャンパス ウエスト1号館 D棟 4階 IMIコンファレンスルーム (W1-D-414)
- 主要言語：日本語
- 共催：九州大学マス・フォア・インダストリ研究所
- 種別・種目：若手・学生研究-短期共同研究
- 研究計画題目：エクパンダーグラフの新しい構成手法の確立とその応用2
- 研究代表者：佐竹 翔平 (熊本大学 半導体・デジタル研究教育機構 総合情報学部門・准教授)
- 研究実施期間：2023年9月4日 (月) ~2023年9月8日 (金)
- 公開期間：2023年9月4日 (月) ~2023年9月5日 (火)
- 研究計画詳細：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2023a017

プログラム

9月4日 (月) 公開

14:00-14:20

冒頭あいさつ・趣旨説明

14:30-15:30

里見 貴志 (東京大学)

Cayleyグラフのエクパンダー性とYoungの畳み込み不等式

15:50-16:50

村松 純 (NTT コミュニケーション科学基礎研究所)

疎グラフ構造を持つ誤り訂正符号

9月5日 (火) 公開

10:30-11:30

Cid Reyes Bustos (NTT基礎数学研究センタ)

Expansion for certain families of non-regular graphs

13:20-14:20

垂井 淳 (電気通信大学)

Expanders and Computational Complexity Theory

14:40-15:40

須賀 祐治 (株式会社インターネットイニシアティブ)

カードベース暗号に見られるアソシエーションスキームについて

16:00-17:00

Semin Oh (Pusan National University)

Finding Graphs with Neural Networks

9月6日 (水) 10:30-17:00 非公開

9月7日 (木) 10:30-17:00 非公開

9月8日 (金) 10:30-15:00 非公開