2024年度共同利用研究報告書

2025年01月10日

所属・職名 三重大学・大学院工学研究科・教授
河内 亮周

		整理番号	2024a006	
1.研究計画題目	情報・計算・暗号の融合による新しい数理基盤の創出			
2.新規・継続	新規			
3.種別	一般研究			
4.種目	研究集会（Ⅱ）			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	河内 亮周		
	所属 部局名	三重大学・大学院工学研究科	職名	教授
7.研究実施期間	2024年09月25日(水曜日)～2024年09月27日(金曜日)			
8.キーワード	情報理論，計算量理論，現代暗号理論			
9.参加者人数	84人			

10.本研究で得られた成果の概要

本研究集会は，高速かつ頑健な通信・計算技術とそれらの安全性の保証する技術の基盤の確立を目指して，情報理論，計算量理論，現代暗号理論の融合に関する最新の成果や知見を研究者間で共有することを目的に開催された．

講演は情報理論，計算量理論，現代暗号理論の最先端および境界領域において第一線で活躍されている国内外の研究者によって行われた．特に10件の講演のうちの研究集会2日目の海外の研究者による招待講演2件を含む5件は英語による講演として，国際的な研究交流を行った．

10件の招待講演は各1時間で実施され，分野としては情報理論分野(3件)，計算量理論分野(4件)，暗号理論分野(3件)と大別できる．さらにそれらの中には情報理論と計算量理論の境界領域，情報理論と統計物理学，機械学習・AIの境界領域，情報理論と計算量理論の境界領域，など融合的研究が数多く含まれていた．全ての招待講演は国際的にトップレベルの学術会議で発表された内容もしくは最先端研究の内容であり，非常に高い水準の発表ばかりであった．質疑応答の時間および休憩時間にも講演者および参加者の間で活発に議論・意見交換が行われており，本研究集会の目的は十分に達成できたと考えられる．

2024年度共同利用研究計画報告書

2024年12月24日

所属・職名 三重大学・大学院工学研究科・教授
河内 亮周

	整理番号	2024a006

1.研究計画題目	情報・計算・暗号の融合による新しい数理基盤の創出	
2.新規・継続	新規	
3.種別	一般研究-研究集会（Ⅱ）	
4.開催方法	ハイブリッド開催	
5.研究代表者	氏名	河内 亮周
	所属・職名	三重大学・大学院工学研究科・教授
6.参加者数	84人	
7.実施期間	2024年9月25日(水)～2024年9月27日(金)	

8.共催

科研費基盤(A) 情報・計算・暗号の融合によるセキュリティ定量化基盤の構築(代表: 安永憲司)
科研費挑戦的研究(開拓) セキュリティ解析の新理論～情報量不等式から計算量不等式へ～ (代表: 渡辺 峻)
Q-LEAP知的量子設計による量子ソフトウェア研究と応用(代表: 藤井 啓祐)

9.組織委員

氏名	所属	職名
わたなべ　しゅん 渡辺 峻	東京農工大学	准教授
やすなが　けんじ 安永 憲司	東京工業大学	准教授
いわもと　みつぐ 岩本 貢	電気通信大学	教授
ぬいだ　こうじ 縫田 光司	九州大学	教授
いけまつ　やすひこ 池松 泰彦	九州大学	助教
きたがわ　ふゆき 北川 冬航	NTT社会情報研究所	准特別研究員

10.本研究で得られた成果の概要

本研究集会は，高速かつ頑健な通信・計算技術とそれらの安全性の保証する技術の基盤の確立を目指して，情報理論，計算量理論，現代暗号理論の融合に関する最新の成果や知見を研究者間で共有することを目的に開催された．

講演は情報理論，計算量理論，現代暗号理論の最先端および境界領域において第一線で活躍されている国内外の研究者によって行われた．特に10件の講演のうちの研究集会2日目の海外の研究者による招待講演2件を含む5件は英語による講演として，国際的な研究交流を行った．

10件の招待講演は各1時間で実施され，分野としては情報理論分野(3件)，計算量理論分野(4件)，暗号理論分野(3件)と大別できる．さらにそれらの中には情報理論と計算量理論の境界領域，情報理論と統計物理学，機械学習・AIの境界領域，情報理論と計算量理論の境界領域，など融合的研究が数多く含まれていた．全ての招待講演は国際的にトップレベルの学術会議で発表された内容もしくは最先端研究の内容であり，非常に高い水準の発表ばかりであった．質疑応答の時間および休憩時間にも講演者および参加者の間で活発に議論・意見交換が行われており，本研究集会の目的は十分に達成できたと考えられる．

参加者についても学部学生からシニア研究者までの幅広い層からの登録があり，参加登録者数は合計84名となった．大学関係者66名，公的研究機関6名，民間企業9名，その他3名であった．特に大学関係者のうち助教・ポスドク・学生の若手が30名と約半数であり，分野の若手育成に大きく貢献できたと考えられる．

偶然であるが，本研究集会の近隣分野の集会として(一般研究-研究集会(I) 2024a030)「情報通信の技術革新のための基礎数理」(研究代表者: 實松豊氏)が同じ会場，同じ日程で開催されており，運営同士で事前に連携体制を整えることができた．聴衆の興味によって両方の研究集会に参加可能できるように調整を行い，さらに懇親会も合同開催とし，結果として分野間の研究交流の幅をより一層広げることができた．

さらには，本研究集会終了直後の9/30に名古屋大学に海外招待講演者2名を招待したポストワークショップを開催して，国際的な研究交流を進めることができた．

本研究集会の開催にあたり，九州大学マス・フォア・インダストリ研究所の共同利用研究計画(一般研究-研究集会(II))ならびに共催の科研費基盤(A) 情報・計算・暗号の融合によるセキュリティ定量化基盤の構築(代表: 安永憲司)，科研費挑戦的研究(開拓) セキュリティ解析の新理論～情報量不等式から計算量不等式へ～ (代表: 渡辺 峻)，Q-LEAP知的量子設計による量子ソフトウェア研究と応用(代表: 藤井 啓祐)の支援を受けた．ここに深く感謝を申し上げる．

11.プログラムおよび講演概要

[2024年9月25日(水)]

13:10-14:10
講演者: 清水 伸高 (東京工業大学)
講演タイトル: 埋め込みクリーク予想とその等価性
概要: 埋め込みクリーク予想とは，大きさkのクリークが埋め込まれたサイズnのランダムグラフにおいて，任意の多項式時間アルゴリズムがサイズ $k \ll \sqrt{n}$ のクリークを見つけることができない，という予想である．このような埋め込みクリーク予想は，探索版で成功確率が指数関数的に1に近い場合，あるいは無視できない成功確率を持つ場合，そして判定版で敵対的に選ばれたkの場合，あるいは二項分布に従って選ばれたkの場合などの数多くの変形版が知られている．本講演では，これらの変形版の予想のほとんどが等価であるという研究成果について述べられた．

14:25-15:25
講演者: 泉 泰介 (大阪大学)
講演タイトル: 2者PSMプロトコルに対する通信複雑性下界の向上
概要: PSMプロトコルとは秘密計算の一種であり，k人の入力を持つ参加者と1人の評価者から構成される暗号プロトコルである．k人の参加者は各自の入力と共有乱数からメッセージを生成し，評価者へ送信する．評価者は予め定められた関数についてそれらのメッセージから参加者の入力に対する関数の出力値を得る．このとき評価者は出力値以外の情報については何も得ることができない．nビット入力を持つ参加者2人でのPSMプロトコルにおいて，既存研究では任意の関数に対してメッセージ長が2^(n/2)ビットという指数関数的な上界とおよそ3nという線形の下界しか知られていなかった．本講演では，この下界を4nに改良するためのアプローチについて解説が行われた．

15:40-16:40
講演者: 和田山 正 (名古屋工業大学)
講演タイトル: 次世代AIアクセラレータに向けた誤り訂正復号法
概要: 前半では勾配流復号法と呼ばれるAIハードウェア向けの誤り訂正復号法について解説が行われた．AIハードウェアでは行列積などを一般化したテンソル計算デバイスが用いられており，そのようなデバイスに適合する誤り訂正復号法を考えることが重要である．本講演では低密度パリティ検査符号に対してテンソル計算による勾配流復号法が提案され，その訂正能力の解析や汎用性が解説された．後半ではスコアベース生成モデルに基づく通信路学習について解説がなされた．通信路モデルがシステム設計時に未知の場合には一般に復号アルゴリズムの設計は困難な問題となるが，近年機械学習技術により通信路を学習する手法が出現している．本講演では勾配流復号法を前提としてその負対数尤度勾配をニューラルネットワークでモデル化し，生成AI分野で注目されているスコアマッチング学習によって通信路を学習し勾配流復号を適用する方式が提案された．

[2024年9月26日(木)]

9:30-10:30
講演者: 三村 和史 (広島市立大学) 遠隔講演
講演タイトル: On Statistical Mechanical Informatics: from Spin Glass to Information Processing
概要: 本講演では，まず情報統計力学と呼ばれる統計力学的手法の情報科学，計算機科学への応用が概観された．さらにその具体例として誤り訂正符号の一つであるSourlas符号の量子復号アルゴリズムとして多体スピングラスモデルのハミルトニアンによる最尤復号法が示されていた．また従来型のHopfieldモデルとモダンHopfieldネットワークの性質の違いが解説され，機械学習分野の Energy Transformer との関係が指摘された．またモダンHopfieldネットワークのひとつである密連想記憶の解析が解説された．

10:45-11:45
講演者: 北川 冬航 (NTT社会情報研究所)
講演タイトル: Cryptographic Primitives with Quantum Secure Key Leasing
概要: 本講演では，量子鍵リースという機能を持つ暗号プロトコルの様々な構成要素についての新しい構成方法と安全性についての研究成果の発表があった．量子鍵リースとは，量子状態を暗号鍵として用いることによって，その鍵が後ほど無効化された際にその無効化されたという事実が検証可能である，という機能である．この機能を持った公開鍵暗号方式の新たな構成方法と安全性証明のアイデアについての解説がなされた．

13:00-14:00
講演者: François Le Gall (名古屋大学)
講演タイトル: Online Locality Meets Distributed Quantum Computing
概要: 本講演では分散計算における量子優位性についての議論がなされた．特にLOCALモデルと呼ばれる一回の通信で送信できる(量子)ビット列の長さに制限がないモデルにおいて，古典LOCALモデルにおいて局所性O(log^*n)で解ける局所検証可能ラベリング問題は定数局所性を持つ有限依存分布を与えることを示した．これは特に正規木の有限依存彩色を与えており，Holroydによる未解決問題への答えを与えている．さらにこのことは分散計算において量子優位性を示すための新たな障壁となりうることが示されていた．

14:15-15:15
講演者: Minki Hhan (Korea Institute for Advanced Study)
講演タイトル: Quantum Complexity for Discrete Logarithms and Integer Factorization
概要: 本講演では，汎用アルゴリズムによる離散対数問題に対する量子計算複雑度の下界証明についての研究成果が示された．古典の暗号理論における計算複雑度の下界証明で用いられる汎用群モデルを拡張した量子汎用群モデルを新たに導入することによって，このモデルの下での群Gに対する離散対数問題を解くために量子アルゴリズムが行う群演算回数の下界がΩ(log|G|)であることが示される．これはShorの離散対数問題に対するアルゴリズムにおける群演算回数とほぼ一致しており，Shorのアルゴリズムのこのモデルの下での最適性を導いている．

15:30-16:30
講演者: Niels Kornerup (The University of Texas at Austin) 遠隔講演
講演タイトル: Quantum Time-Space Tradeoffs for Matrix Problems
概要: 本講演では，行列-行列積や行列-ベクトル積などの行列に関連する広い範囲の問題を解く量子アルゴリズムについて必要な質問回数とメモリ量のトレードオフの下界解析が議論された．またブール行列積問題について必要な質問回数とメモリ量の間の既存のトレードオフを改良する下界を証明している．この新しい下界証明においてはZhandryの量子質問記録に基づいた振幅バケット法という強力な証明技術が導入されていた．

[2024年9月27日(金)]

9:30-10:30
講演者: 葛岡 成晃 (和歌山大学)
講演タイトル: 推測とデータ圧縮，および関連する話題
概要: 副次情報付きの推測問題において推測者の正解するまでの推測回数のモーメントの上下界が条件付きRenyiエントロピーで特徴付けられることがArikanによって示されている．推測者が途中で推測を諦めてもよい推測問題の亜種を考える．その推測回数のモーメントの上下界がWolfとRennerによって与えられたものとは異なる新たな平滑化Renyiエントロピーを導入することで，その亜種に対する推測回数のモーメント上下界を特徴付けた講演者の成果が紹介された．また別の応用として副次情報付き可変長情報源符号化の符号長を指数部とするモーメントの上下界が新たに導入された平滑化Renyiエントロピーによって特徴付けられることを示していた．

10:45-11:45
講演者: 渡辺 峻 (東京農工大学)
講演タイトル: ビットセキュリティと困難性増幅における情報理論の役割
概要: ビットセキュリティとは暗号学的なシステムが持つ安全性を定量化したものである．一方向性などを定量化する探索問題型のビットセキュリティを踏まえた上で，識別不可能性などを定量化する判定問題型のビットセキュリティはMicciancioとWalterによって定義されていたが，その操作論的な意味が明確ではなかった．本講演では，判定問題型のビットセキュリティを操作論的に定義し，Micciancio-Walterの定義との等価性を示した．またその応用としてビットセキュリティを保つブール関数の困難性増幅の構成法を与えた．

開催日：2024/09/25～2024/09/27

情報・計算・暗号の融合による新しい数理基盤の創出｜2024a006

カテゴリー：イベント　タグ：一般研究　研究集会II

開催概要

- **開催方法**：Zoomミーティングによるハイブリッド開催
- **開催場所**：JR博多シティ9階会議室(1)
- **主要言語**：日本語（9/25，9/27）英語（9/26）
- **共催**：九州大学マス・フォア・インダストリ研究所、科研費基盤(A) 情報・計算・暗号の融合によるセキュリティ定量化基盤の構築 (代表: 安永 憲司)、科研費
セキュリティ解析の新理論～情報量不等式から計算量不等式へ～ (代表: 渡辺 峻)、Q-LEAP知的量子設計による量子ソフトウェア研究開発と応用 (代表:
- **種別・種目**：一般研究-研究集会（Ⅱ）
- **研究計画題目**：情報・計算・暗号の融合による新しい数理基盤の創出
- **研究代表者**：河内 亮周（三重大学・大学院工学研究科・教授）
- **研究実施期間**：2024年9月25日（水）～2024年9月27日（金）
- **公開期間**：2024年9月25日（水）～2024年9月27日（金）
- **研究計画詳細**：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2024a006

プログラム

9月25日（水）13:00-16:40

13:00-13:10

開会の挨拶

13:10-14:10

清水 伸高 (東京工業大学)

埋め込みクリーク予想とその等価性

14:25-15:25

泉 泰介 (大阪大学)

2者PSMプロトコルに対する通信複雑性下界の向上

15:40-16:40

和田山 正 (名古屋工業大学)

次世代AIアクセラレータに向けた誤り訂正復号法

9月26日（木）9:30-16:30

9:30-10:30

三村 和史 (広島市立大学)

On Statistical Mechanical Informatics: from Spin Glass to Information Processing

- **10:45-11:45**

北川 冬航 (NTT社会情報研究所)

Cryptographic Primitives with Quantum Secure Key Leasing

- **13:00-14:00**

François Le Gall (名古屋大学)

Online Locality Meets Distributed Quantum Computing

- **14:15-15:15**

Minki Hhan (Korea Institute for Advanced Study)

Quantum Complexity for Discrete Logarithms and Integer Factorization

- **15:30-16:30**

Niels Kornerup (The University of Texas at Austin)

Quantum Time-Space Tradeoffs for Matrix Problems

9月27日（金）9:30-11:55

- **9:30-10:30**

葛岡 成晃 (和歌山大学)

推測とデータ圧縮，および関連する話題

- **10:45-11:45**

渡辺 峻 (東京農工大学)

ビットセキュリティと困難性増幅における情報理論の役割

- **11:45-11:55**

閉会の挨拶

現地参加者向けの懇親会を以下の要領で開催予定です．

なお懇親会は研究集会「情報通信の技術革新のための基礎数理」(https://joint.imi.kyushu-u.ac.jp/post-14984/)との合同開催です．

懇親会参加ご希望の方は9/11(水)までに懇親会参加登録ページよりお申込み下さい．

なお9/11(水)までに参加ご希望の方の数が会場のキャパシティを超える場合には
参加募集を早期に終了する可能性があります．予めご承知おき下さい．

日時：9/26(木) 18:00〜 2時間
会場：炙り炉端 山尾 博多駅前（JR博多駅 徒歩5分）
https://tabelog.com/fukuoka/A4001/A400101/40036193/
参加費: 5,000円

懇親会参加登録サイトはこちら(https://docs.google.com/forms/d/e/1FAIpQLSdh_x5RGrYq7l0cLyGutKxRZlSxgdYB9zd_vl7V3ejvIDYLYg/viewform?us

申込方法

事前申込制（組織委員，講演者のかたも登録が必要です）
参加無料
定員になり次第，参加登録を締め切らせていただく場合がございます．

＼下記URLより参加登録をお願いいたします／

参加登録フォーム

Zoom（オンライン）からご参加の方

Zoomを使ったオンライン開催，ハイブリッド開催の場合

参加登録後に件名［九大IMIより］Zoom用URLのお知らせというメールがimikyoten@gmail.comから自動配信されます．
届いていない方は，お手数をおかけしますがもう一度ご登録いただくか下記にメールにてご連絡をお願い申し上げます．
（迷惑メールフォルダもご確認お願いいたします）

＜九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点事務室＞
imikyoten(at)jimu.kyushu-u.ac.jp
(at)を@に変更してください

Zoomについて

開催日までにZoomアプリをインストールしてください．
Zoomアプリは無料版で問題なくご視聴いただけます．

ミーティング用Zoomクライアントのダウンロードは下記からお願いします．
すでにインストールされている方は最新版にアップデートをお願いいたします．
https://zoom.us/download#client_4meeting

パソコンやスマホへのインストール方法は下記をご参照ください．
https://zoom.nissho-ele.co.jp/blog/manual/zoom-install.html