

情報工学専攻	コンピュータサイエンス講座	(コンピュータソフトウェア研究室)	
教員構成	教授・河内亮周	講師・山田俊行	特任助教・RAY Maharshi

I. 現在の研究テーマ、研究内容

1. キーワード

量子情報科学, 計算の理論, 情報セキュリティ, 現代暗号理論
自動推論, 組み合わせ最適化, ソフトウェアの解析と検証, プログラム理解支援

2. 研究テーマ

“量子情報科学”

量子計算・量子通信を用いて既存の技術では実現できないような情報処理を達成する方法について模索する.

“計算の理論”

計算機で解くのが困難な問題の計算量を解析し, 計算の原理的な限界を明らかにする.

“情報セキュリティ”

情報ネットワークにおける暗号通信プロトコルの設計および安全性の解析を行う.

“ソフトウェア解析”

空ポインタ参照など、実行時の不正処理が行われるかどうかをプログラムを解析することで実行前に検出する研究を行う.

“プログラム理解支援”

開発者や学習者が必要な、プログラムに関する情報を抽出し、わかりやすく提示する研究を行う.

II. 研究活動

1. 口頭発表

●国際会議

- (1) The 2021 IEEE Information Theory Workshop (2021 年 10 月 17 日-21 日) オンライン開催
“Recent Progress in Private Simultaneous Messages Protocols” Akinori Kawachi

●国内学会

- (1) Q-LEAP 量子 AI 国内研究会 (2021 年 9 月 9 日-10 日) オンライン開催
“アルゴリズム理論・計算量理論による量子計算/通信の優位性理解に向けて”
○河内 亮周
(2) 研究集会 「量子暗号理論と耐量子暗号」 (2022 年 3 月 18 日) オンライン開催
“秘密同時通信における近年の進展について”
○河内 亮周

●その他

- (1) QLEAP Theory Seminar オンライン開催
“Communication complexity of private simultaneous quantum messages protocols” Akinori Kawachi

2. 著書

- (1) “理論計算機科学事典” 朝倉書店 (2022 年 1 月 1 日) p.18
河内 亮周 (単著または編著) ISBN : 978-4-254-12263-3

3. 学術論文

●原著論文 (査読のあるもの)

- (1) “Communication Complexity of Private Simultaneous Quantum Messages Protocols”
Akinori Kawachi, and Harumichi Nishimura (July 2021)
Proceedings of the 2nd International Conference on Information-Theoretic Cryptography
[pp.20:1~20:19]
- (2) “A Commitment Scheme with Output Locality-3 fit for the IoT Device”
Hideaki Miyaji, Yuntao Wang, Akinori Kawachi, and Atsuko Miyaji (November 2021)
Security and Communication Networks [2021, pp.1~10]
- (3) “機械の種類を考慮した調理手順最適化の値範囲と big-M 法を用いた離接制約の比較”
石野ちあき, 森本尚之, 山田俊行 (2021 年 8 月)
情報処理学会論文誌：数理モデル化と応用(TOM59) [14(3), pp.85~92]
- (4) “手続きを含む命令型プログラムを検証するための証明戦略の提案”
小島裕登, 山田俊行 (2021 年 6 月)
情報処理学会論文誌：プログラミング(PRO) [14(3), pp.1882~7802]

●国際会議の Proceedings

- (1) “Communication Complexity of Private Simultaneous Quantum Messages Protocols”
Proceedings of the 2nd International Conference on Information-Theoretic Cryptography (July 2021)
[pp.20:1~20:19] Akinori Kawachi
- (2) “Recent Progress in Private Simultaneous Messages Protocols”
Proceedings of 2021 IEEE Information Theory Workshop (October 2021) Akinori Kawachi
- (3) “線形交差エントロピー試験を突破する古典アルゴリズムの実験的解析” (2021 年 5 月)
河内 亮周 電子情報通信学会技術研究報告 [vol. 121, no. 11, pp.46~53]
- (4) “Fan-out ゲート付きの浅層量子回路の計算能力” (2021 年 12 月)
河内 亮周 電子情報通信学会技術研究報告 [vol. 121, no. 285, pp.24~29]
- (5) “Even-Mansour 暗号に対する量子攻撃の最適性” (2022 年 2 月)
河内 亮周 2021 年度冬の LA シンポジウム [S1]
- (6) “Randomness Bounds for Private Simultaneous Messages and Conditional Disclosure of Secrets”
(2022 年 2 月) 河内 亮周 2021 年度冬の LA シンポジウム [12, pp.12-1~12-38]

4. その他の研究成果

なし

5. 学会賞等

Even-Mansour 暗号に対する量子攻撃の最適性 (三重大学大学院工学研究科)
河内 亮周 2 位 (三重大学学生総合支援機構)

6. 新聞記事等

なし

Ⅲ. 研究費関係

1. 文部科学省科学研究費

- (1) 基盤研究 (C) 「より現実的なネットワークモデルにおける効率的な秘密計算プロトコルの設計と解析」 (代表・河内 亮周・新規・課題番号 21K11887) 650 千円
- (2) 基盤研究 (A) 「量子情報化社会に向けた量子計算基盤の構築」
(分担, 小柴 健史・新規・課題番号 21H04879) 700 千円
- (3) 基盤研究 (B) 「インセンティブを考慮した暗号基盤技術の構築」
(分担・河内亮周・継続・課題番号 17H01695) 440 千円
- (4) 若手研究(B) 「計算内在暗号化技術の計算モデル」
(代表・河内亮周・継続・課題番号 17K12640) 245 千円

2. 他省庁・財団からの基金

- (1) 文部科学省 令和2年度光・量子飛躍フラッグシッププログラム (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」
(分担・河内亮周・新規) 10,352千円

3. 民間等との共同研究・受託研究

なし

4. 奨学寄附金

なし

Ⅳ. 国際交流

●外国人留学生の受入

なし

Ⅴ. その他

なし

個人資料

教授・河内亮周

●所属学協会及び役員・委員等

文部科学省 科学技術政策研究所科学技術動向研究センター・専門調査員 (2013 年～)

電子情報通信学会・量子情報技術時限専門委員会・委員 (2010 年～)

北陸先端科学技術大学院大学 大学院教育イニシアティブセンター・サポートメンバー
(2010 年～)

電子情報通信学会・離散数学とその応用小特集編集委員会・編集委員 (2007 年～)

電子情報通信学会・英文論文誌理論計算機科学小特集編集委員会・編集委員 (2021 年)

The 32nd International Symposium on Algorithms and Computation・Program Committee
(2021 年)

電子情報通信学会・英文論文誌小特集離散数学とその応用編集委員会・編集副委員長
(2021 年)

工学研究科広報委員会・委員長 (2021 年)

工学研究科入試委員会・副委員長 (2021 年)
工学研究科学生委員会・委員長 (2021 年)
AC 選抜方法開発・実施部門会議・委員 (2021 年)
学生なんでも相談室分室 (2021 年)
AC 高大接続部門会議 (2021 年)
工学研究科学生委員会・情報工学コース委員 (委員長と兼任) (2021 年)
情報工学コース・情報工学専攻就職担当 (2021 年)
(秘匿が求められている委員活動)・大学入学共通テスト第 7 試験場主任 (2021 年)

●国内・国際会議等の役員・委員等
なし

●官公庁・民間団体等の委員等
なし

●その他
独立行政法人 日本学術振興会 (秘匿が求められている委員活動) 委員 (2021 年)
独立行政法人 日本学術振興会 (秘匿が求められている委員活動) 委員 (2020 年～2021 年)
独立行政法人 日本学術振興会 (秘匿が求められている委員活動) 委員 (2021 年～2022 年)

講師・山田俊行

●所属学協会及び役員・委員等
日本ソフトウェア科学会 (1994 年～)
情報処理学会 (2017 年～)
情報処理学会・情報処理学会 東海支部 運営委員会・運営委員 (2020 年～2022 年)
(秘匿が求められている委員活動) (2021 年)
自己点検・評価委員会 (2021 年度)
クラス担任 (4 年) (2021 年度)
(秘匿が求められている委員活動) (2021 年)
(秘匿が求められている委員活動) (2021 年)

●官公庁・民間団体等の委員等
なし

特任助教・RAY Maharshi

●所属学協会及び役員・委員等
なし