

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,
自動推論, 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) International Symposium on Information Theory and Its Applications (ISITA 2020), (October 24-27, 2020), Kapolei, Hawai'i, USA (Online Events)

“Hamming Weight of Product of Random Sparse Polynomials”

○Akinori Kawachi

●国内学会

(1) 令和2年度電気・電子・情報関係学会東海支部連合大会 (2020年9月3日-4日) オンライン開催

“規則の辞書を用いたプログラム例からの文法の推測”

○毛利真士, 山田俊行

(2) 情報処理学会第131回数理モデル化と問題解決研究発表会 (2020年12月17日-18日) オンライン開催

“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

(3) 情報処理学会第132回プログラミング研究会 (2021年1月13日-14日) オンライン開催

“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術の提案”

- 小島裕登, 山田俊行
- (4) The 38th Symposium on Cryptography and Information Security (SCIS2021)
暗号と情報セキュリティシンポジウム, (January 19-22, 2021), 3A2-3, Online.
“秘密同時メッセージと条件付き秘密開示に対する乱数長下界”
○河内 亮周, 吉田 真紀 (情報通信研究機構)
- (5) 2020 年度冬の LA シンポジウム (2021 年 2 月 1 日-3 日) オンライン開催
“量子秘密同時メッセージプロトコルの通信計算量”
○河内亮周, 西村治道 (名古屋大学)
- (6) 第 23 回プログラミングおよびプログラミング言語ワークショップ (2021 年 3 月 9 日-11 日) オンライン開催
“文法の規則集の編集によるプログラム例からの文法の生成とその実装”
○毛利真士, 山田俊行
- (7) 2021 年電子情報通信学会総合大会企画セッション「量子計算と暗号の進展」
依頼シンポジウム講演 (2021 年 3 月 9 日-12 日) オンライン開催
“量子攻撃者に対する安全性証明技術の進展”
○河内亮周

●その他

- (1) 京都大学基礎物理学研究所量子情報ユニット主催第三回量子情報スクール, 招待講演
2020 年 6 月 30 日, オンライン開催
“ (量子) 回路計算量の下界証明”
○河内 亮周
- (2) 北陸先端科学技術大学院大学 第一回情報科学系セミナー, 2020 年 8 月 6 日, オンライン
開催
“Shor のアルゴリズム短期集中講座”
○河内 亮周
- (3) The 10th International Symposium for Sustainability by Engineering at Mie University (Research
Area C) (Sept. 24-25, 2020) MIE UNIV.(Online Conference Event via Zoom)
“Disjunctive Constraints Using Integer Range for Food Preparation Scheduling”
○Chiaki Ishino, Toshiyuki Yamada, and Naoyuki Morimoto
- (4) The 10th International Symposium for Sustainability by Engineering at Mie University (Research
Area C) (Sept. 24-25, 2020) MIE UNIV.(Online Conference Event via Zoom)
“Route search according to service usage frequency and value”
○Tomohiko Kumagai and Toshiyuki Yamada
- (5) The 10th International Symposium for Sustainability by Engineering at Mie University (Research
Area C) (Sept. 24-25, 2020) MIE UNIV.(Online Conference Event via Zoom)
“Coq Tactics for Verifying Imperative Programs with Functions”
○Hiroto Kojima and Toshiyuki Yamada
- (6) The 10th International Symposium for Sustainability by Engineering at Mie University (Research
Area C) (Sept. 24-25, 2020) MIE UNIV.(Online Conference Event via Zoom)
“Example-Guided Grammar Generation Using a Grammar Dictionary”
○Masato Mouri and Toshiyuki Yamada

2. 著書

- (1) Security Infrastructure Technology for Integrated Utilization of Big Data: Springer Open,
ISBN 978-981-15-3654-0 (eBook), Chapter 3, pp.35-63, 23 April 2020.

"Secure Primitive for Big Data Utilization"

Akinori Kawachi, Atsuko Miyaji, Kazuhisa Nakasho, Yiyi Qi, and Yuuki Takano

3. 学術論文

●原著論文（査読のあるもの）

(1) Physical Review A 103, 012418, Iss. 1 (25 January 2021)

"Quantum algorithms for hedging and the learning of Ising models"

Patrick Reberntrost, Yassine Hamoudi, Maharshi Ray, Xin Wang, Siyi Yang, Miklos Santha

(2) New Journal of Physics, Vol. 23, 033006 (5 March 2021)

"Graph-theoretic approach to dimension witnessing"

Maharshi Ray, Naresh Goud Boddu, Kishor Bharti, Leong-Chuan Kwek, and Adan Cabello

●国際会議の Proceedings

(1) Proceedings of 2020 International Symposium on Information Theory and Its Applications (ISITA 2020), pp.368-371, 2020.

"Hamming Weight of Product of Random Sparse Polynomials"

Akinori Kawachi

4. その他の研究成果

なし

5. 学会賞等

なし

6. 新聞記事等

(1) 夢ナビ TALK(夢ナビライブ名古屋会場), 2020年7月, 広報資料ウェブ掲載
"未来を創る量子情報技術"

河内 亮周

III. 研究費関係

1. 文部科学省科学研究費

(1) 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) 700 千円

(2) 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) 600 千円

(3) 基盤研究(A) 「量子プロトコル理論の線的展開」

(分担・河内亮周・継続・課題番号 16H01705) 600 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) 10,000千円

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

(1) 中国・研究生 (2020年10月～2021年3月)

“オンラインストレージを利用する人々の個人情報を守るセキュリティキーシステムの開発”

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

- ・ 情報処理学会・正会員
- ・ 電子情報通信学会・正会員
- ・ LA シンポジウム・会員

●その他

- ・ 北陸先端科学技術大学院大学 非常勤講師 (2020年8月)
- ・ 大阪大学大学院工学研究科 招へい教員 (2019年4月～2021年3月)
- ・ 大阪大学先導的学際研究機構 招へい教員 (2019年4月～2021年3月)

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・正会員
- ・ 情報処理学会・正会員
- ・ 情報処理学会東海支部委員 (2020年4月～)

●官公庁・民間団体等の委員等

- ・ 放送大学三重学習センター 非常勤講師 (2020年10月～2021年3月)
- ・ 川越町 地域公共交通検証事業に関するアドバイザー (2020年8月～2021年3月)

特任助教・RAY Maharshi

●所属学協会及び役員・委員等