

基本情報

学科名 講座名 (研究室名)

情報工学専攻 コンピュータサイエンス

教員構成 職名・氏名 (河内 亮周)

I. 現在の研究テーマ、研究内容

1. キーワード

2. 研究テーマ

研究内容

II. 研究活動[欧文は原文で記入する。]

1. 口頭発表

●国際会議

RE:BIT 2022 (202208) Hawaii, U.S.A. “Proof Techniques for Quantum Query Lower Bounds (or How to Evaluate the Amount of Information from Oracles by Quantum Queries)”

Akinori Kawachi

IWSEC 2022 東京 “Secure Multi-party Computation for Symmetric Function with Tree Interaction Patterns” Miho Miyake and Akinori Kawachi

●国内学会

第5回金沢暗号理論勉強会 (202206) 金沢大学サテライト・プラザ “量子情報の基礎” 河内 亮周

第5回金沢暗号理論勉強会 (202206) 金沢大学サテライト・プラザ “量子質問計算量の上界” 河内 亮周

第5回金沢暗号理論勉強会 (202206) 金沢大学サテライト・プラザ “量子質問計算量の下界” 河内 亮周

2022年度夏のLAシンポジウム 秋田 “木状相互通信パターンにおける対称関数に対する秘密計算プロトコル” 三宅 美歩, 河内 亮周

2022年度夏のLAシンポジウム 秋田 “二元体上算術回路に対する乱択符号化の符号長の改

良” 西窪 勇人, 河内 亮周

電気・電子・情報関係学会 東海支部連合大会 (202208) オンライン “Paillier 暗号による安全な連合学習の計算量削減の実験の評価” XU SHILIN, 河内 亮周

2023 年情報とセキュリティシンポジウム (202301) リーガロイヤルホテル小倉 “木状相互通信パターンにおける秘密計算プロトコル” 三宅 美歩, 縫田 光司, 河内 亮周

2022 年度冬の LA シンポジウム (202301) 京都大学数理解析研究所 “線形リスト探索に対する量子質問計算量の下界” 酒井 裕太郎, 河内 亮周

2022 年度冬の LA シンポジウム (202301) 京都大学数理解析研究所 “耐量子計算機暗号 HQC の復号誤り確率の解析の改良” 山口 耕平, 河内 亮周

2022 年度冬の LA シンポジウム (202301) 京都大学数理解析研究所 “確率的対数領域計算による確率行列のスペクトルギャップ増幅” 鈴木 健介, Maharshi Ray, Francois Le Gall, 河内 亮周

●その他

大阪大学情報科学研究科量子勉強会第 2 回 (202301) 大阪大学吹田キャンパス “量子情報科学から見た Bell 不等式の破れ” 河内 亮周

ノーベル物理学賞解説講演会 (202211) 三重大学 “2022 年ノーベル物理学賞解説 ベル不等式の破れと量子情報科学” 河内 亮周

2. 著書

3. 学術論文

●原著論文 (査読のあるもの。)

“Proof Techniques for Quantum Query Lower Bounds (or How to Evaluate the Amount of Information from Oracles by Quantum Queries)” Akinori Kawachi RE:BIT 2022 [pp.16~16 (202208)]

●国際会議の Proceedings

“Proof Techniques for Quantum Query Lower Bounds (or How to Evaluate the Amount of Information from Oracles by Quantum Queries)” 河内 亮周 RE:BIT 2022 [pp.16~16(202208)]

“二元体上算術回路に対する乱択符号化の符号長の改良” 河内 亮周 2022 年度夏の LA シンポジウム [pp.S15-1~S15-2(202207)]

“木状相互通信パターンにおける対称関数に対する秘密計算プロトコル” 河内 亮周 2022 年度夏の LA シンポジウム [pp.S5-1~S5-2(202207)]

“Paillier 暗号による安全な連合学習の計算量削減の実験の評価” 河内 亮周 2022 年度電気・電子・情報関係学会 東海支部連合大会 [G2-4, (2022)]

“木状相互通信パターンにおける秘密計算プロトコル” 河内 亮周 2023 年暗号と情報セキュリティシンポジウム [pp.1~8(202301)]

“線形リスト探索に対する量子質問計算量の下界” 河内 亮周 2022 年度冬の LA シンポジウム [pp.S7-1~S7-10(202301)]

“耐量子計算機暗号 HQC の復号誤り確率の解析の改良” 河内 亮周 2022 年度冬の LA シンポジウム [pp.S10-1~S1-⁵(202301)]

“確率的対数領域計算による確率行列のスペクトルギャップ増幅” 河内 亮周 2022 年度冬の LA シンポジウム [pp.S12-1~S12-7(202301)]

●総説, 解説等

●その他

4. その他の研究成果 (作品, 設計, 発明・特許)

5. 学会賞等

Miho Miyake and Akinori Kawachi, “Secure Multi-party Computation for Symmetric Function with Tree Interaction Patterns” Best Poster Award (IWSEC 2022)

6. 新聞記事等

III. 研究費関係

1. 文部科学省科学研究費

科学研究費 (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・工学研究科・継続・21K11887) 650 (千円)

科学研究費 (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・継続・21H04879) 780 (千円)

2. 省庁・財団からの基金

3. 民間等の共同研究・受託研究

4. 奨学寄附金

IV. 国際交流

- 海外出張・研修

河内 亮周・ハワイ (20220826～20220831) 学会参加

- 海外大学等での講演など

河内 亮周・工学研究科・Hawaii, USA (202208) “RE:BIT 2022”

- 外国人研究者の受入れ

- 外国人研究者の訪問

- 外国人留学生の受入れ

- 外国人との共同研究

V. その他

- 他大学等公的機関との共同研究

- 大学内での共同研究

個人資料

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 (2013～2017)

電子情報通信学会・量子情報技術時限専門委員会・委員 (2010～)

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 (2007～2021)

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・編集副委員長 (2022～2022)

工学部入試委員会・副委員長 (2022～2022)

入試委員会・委員 (2022～2022)

工学部学生委員会・委員長（2022～2022）

学生委員会・委員（2022～2022）

AC 選抜方法開発・実施部門会議（2022～2022）

AC 高大接続部門会議・委員（2022～2022）

工学部広報委員会・委員長（2022～2022）

学生なんでも相談室（2022～2022）

障害学生支援調整会議（2022～2022）

●国内・国際会議等の役員・委員等

●官公庁・民間団体等の委員等

●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 委員（2021～2022）

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 委員（2021～2022）

基本情報

学科名 講座名 (研究室名)
情報工学専攻 コンピュータサイエンス

教員構成 職名・氏名 (山田 俊行)

I. 現在の研究テーマ、研究内容

1. キーワード

計算論理, 組み合わせ最適化, プログラム理解支援, ソフトウェアの解析と検証

2. 研究テーマ

計算論理, ソフトウェアの 解析・理解支援・検証, 組み合わせ最適化

研究内容

II. 研究活動[欧文は原文で記入する。]

1. 口頭発表

●国際会議

●国内学会

電気・電子・情報関係学会東海支部連合大会 (202208) オンライン “SVM と伝搬ネットワークを用いた誹謗ツイートの検出” 加藤将志, 山田俊行

電気・電子・情報関係学会東海支部連合大会 (202208) オンライン “精度保証を含むプログラム間の動作の等価性のための同値遷移システム” 近藤流司, 山田俊行

●その他

International Symposium for Sustainability by Engineering at MIU 2020 (202209) オンライン “Improving Coverage of Slanderous Tweet

Detection Using SVM and Propagation Network” Masashi Kato and Toshiyuki Yamada

International Symposium for Sustainability by Engineering at MIU 2020 (202209) オンライン “Interval Transition System : Ensuring Accuracy of Program Execution” Ryuji Kondo and Toshiyuki Yamada

三重大学と地元企業の連携セミナー (202212) “製造工程やバス運行経路の最適化～より良い組み合わせの探索” 山田俊行

2. 著書

3. 学術論文

●原著論文（査読のあるもの。）

●国際会議の Proceedings

●総説, 解説等

●その他

“SVM と伝搬ネットワークを用いた誹謗ツイートの検出” 山田 俊行 2022 年度電気・電子・情報関係学会東海支部連合大会講演論文集 [(202208)]

“精度保証を含むプログラム間の動作の等価性のための同値遷移システム” 山田 俊行 2022 年度電気・電子・情報関係学会東海支部連合大会講演論文集 [(202208)]

4. その他の研究成果（作品, 設計, 発明・特許）

5. 学会賞等

6. 新聞記事等

III. 研究費関係

1. 文部科学省科学研究費

2. 省庁・財団からの基金

3. 民間等の共同研究・受託研究

共同研究「電子部品実装機における動作プログラムの最適化」 株式会社 FUJI
1,000（千円）

共同研究「地域公共交通検証事業（ふれあいバス運行に関するデータ分析および経路最適化）」川越町 715（千円）

4. 奨学寄附金

IV. 国際交流

- 海外出張・研修
- 海外大学等での講演など
- 外国人研究者の受入れ
- 外国人研究者の訪問
- 外国人留学生の受入れ
- 外国人との共同研究

V. その他

- 他大学等公的機関との共同研究
共同研究「地域公共交通検証事業（ふれあいバス運行に関するデータ分析および経路最適化）」川越町
- 大学内での共同研究

個人資料

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～)

情報処理学会 (2017～)

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～
2022)

入試委員会 (2022～2022)

●国内・国際会議等の役員・委員等

●官公庁・民間団体等の委員等

●その他