様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月　 １ 日現在

機関番号：１３９０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０４０６６

研究課題名（和文）対話型証明の新展開－古典から量子まで

研究課題名（英文）New Developments in Interactive Proofs - From Classical to Quantum

研究代表者
西村　治道（Nishimura, Harumichi）

名古屋大学・情報学研究科・教授

研究者番号：７０４３３３２３

交付決定額（研究期間全体）：（直接経費）　　11,300,000円

研究成果の概要（和文）：対話型証明とは，原理的に無限の計算能力をもつ証明者と呼ばれるパーティと多項式時間（効率的に実行できるとされる時間）で計算を行うことしかできない検証者と呼ばれるパーティが対話をすることにより，検証者が検証可能となる計算問題を研究する計算モデルである．本研究課題では対話型証明やその量子計算版である量子対話型証明について，経済的な概念を導入したモデルや検証者がネットワークであるような新しい形のモデルを導入し，これらによって効率的に検証可能な問題が何かを計算量理論や量子情報理論の技術を利用して解析した．

研究成果の学術的意義や社会的意義
本研究課題で得られた対話型証明および量子対話型証明の新しい展開に対する知見は，対話型証明という基本的で重要な計算モデルが計算問題の検証における理論的な可能性と限界に対する理解を推し進めるものである．特に，経済的合理性や検証者がネットワーク上に分散的に存在することといった量子対話型証明に対する概念的拡張は本研究課題ではじめて提案され，その理論的な礎が築かれた．本研究課題の成果が対話型証明によって効率的に検証可能な計算問題に関する多層的な解明につながることが今後のさらなる研究によって期待される．

研究成果の概要（英文）：Interactive proofs are computational models that study computational problems that can be verified by a party called the verifier, who has in principle infinite computational power, and a party called the verifier, who can only perform the computation in polynomial time (time that is considered to be efficiently executable), through interactive communication. In this research project, we introduced a new model for interactive proofs and its quantum computational version, quantum interactive proofs, in which the verifier is a network or a model that introduces an economic concept, and analyzed which problems can be efficiently verified by these models using techniques of computational complexity theory and quantum information theory.

研究分野：量子計算，計算量理論

キーワード：対話型証明　量子計算　計算量理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

対話型証明とは与えられた問題の正しさを効率的に検証するための計算モデルであり，1980 年代半ばにゼロ知識証明の概念の定式化や群論的な問題の効率的検証を目的として導入された．対話型証明では，検証者とよばれる効率的（多項式時間乱択）アルゴリズムだけが実行できるパーティと，証明者と呼ばれる計算能力無限だが必ずしも正直ではないパーティが通信を行い，検証者が問題の正しさを検証できるようなプロトコルの構築を目指す．対話型証明の枠組みは今日の計算量理論において最重要なものの一つである．証明者の人数が複数となったモデル（多証明者対話型証明）など様々な種類の対話型証明モデルが提案・研究され，ゼロ知識証明を始めとする暗号理論における数々のプロトコルや確率検査証明と近似アルゴリズムの限界への応用といった形で，理論計算機科学を下支えしている．

量子コンピュータは研究開始当初の数年前から国内外で急速に注目を集めていてそれは現在でも継続中である．Google や IBM といった企業が量子コンピュータの開発に注力し，小規模ながらもクラウドでの利用ができるようになったこともあって各種メディアで話題に挙がり，国内でも Q-LEAP のような大規模プロジェクトが始まった．一方で，量子コンピュータの計算原理である量子計算は，対話型証明と同じく 1980 年代に Feynman や Deutsch によって提唱・モデル化され，その計算量理論（量子計算量理論）も Vazirani や Yao によって端緒が切られた．量子計算量理論は当初ほとんど注目されていなかったが，1990 年代に Shor や Grover による量子計算を利用したアルゴリズム（量子アルゴリズム）が開発され，従来の古典計算（以下，従来の計算は量子との対比で古典と呼ぶ）に対する計算効率の幾つかの優位性が理論的に明らかになって以降，量子情報科学におけるコアトピックとして着実に研究が進められていた．

対話型証明は量子計算量理論においても以下の二つの観点から重要な研究対象である．第一はその量子版の研究である．量子対話型証明は，対話型証明における検証者の計算や通信を量子計算や量子通信に置き換えた量子計算モデルの一つである．任意のプロトコルで検証可能な問題のクラスが３回の通信で検証可能なクラスと等しいという古典の対話型証明では予想されていないような結果[Kitaev，Watrous，STOC2000，pp.608-617]や，多証明者量子対話型証明と量子力学における Bell の不等式との関連が明らかになるにつれ，この量子計算モデルは古典の対話型証明とは違った形で注目を集め，計算機科学だけでなく物理や情報の研究者もその計算能力や特性などを精力的に探究している．第二は近年の量子コンピュータのクラウド利用に動機づけられた量子コンピュータの検証問題である．この問題では量子コンピュータを持つと主張するサーバに対して古典コンピュータしか持たないクライアントが量子コンピュータを用いた計算を委託するとき，本当に量子コンピュータを使って計算しているかを検証する問題である．この問題は古典の対話型証明において正直な証明者の計算能力が多項式時間の量子計算に制限された計算モデルとして定式化でき，非常に重要度の高い未解決問題である．

２．研究の目的

本研究は互いに関連する以下の目的を持っている．

(A) 量子コンピュータの検証問題の基盤となる対話型証明のより良い方向性の追究
(B) 量子通信・量子計算・量子もつれが制限された対話型プロトコルの検証能力の解明
(C) 多人数が関係する対話型プロトコルの検証能力の解明

(A)は完全に古典の対話型証明をターゲットとする．量子コンピュータの検証問題の究極的な問いは，対話型証明の言葉では以下のようになる．正直な証明者は多項式時間の量子計算を行う能力を持ち，検証者は多項式時間の古典計算の能力しか持たない対話型証明モデルにおいて，多項式時間の量子計算で解けるすべての問題が検証できるのか？ 15 年以上にわたる様々な研究者の努力にもかかわらず現時点でこの問いの完全解決は非常に困難であるため，検証者が非常に限定された量子計算を許された場合や，量子状態を予め共有した複数の証明者が存在するという多証明者量子対話型証明の場合などで検証可能という報告がなされている．本研究ではゲーム理論的な要素を持つ対話型証明のモデルとして，合理的証明と呼ばれる計算モデルに着目し，そのモデルのもとでの解決を目指す．

(B)は半量子・半古典ともいえる対話型プロトコルをターゲットとする．既に述べた通り量子通信に何の制限もなければ量子対話型証明における通信回数は３回で十分である．しかし，量子通信は古典通信に比べて技術的にも経済的にも高コストであり，量子通信を古典あるいは簡単な量子状態生成のみを用いたものに制限できればその方が望ましい．また，量子計算も現状を鑑みると，近未来的には機能が制限された量子計算モデルをベースとすることも検討する必要がある．そこで本研究では，量子通信や検証者，証明者の量子計算が制限された対話型プロトコルの計算量理論的基盤を整備し，その検証能力について詳細な解析を行う．

目的(C)では多人数からなるような対話型プロトコルをターゲットとする．例えば，検証者の人数が多数である場合，それらの検証者はネットワーク上の各ノードであり，ノード間の通信は制約的である．このような状況において効率的な検証が可能な計算問題が何かを研究することは，分散計算の分野において 2000 年代に提唱され，活発に研究がなされている．本研究課題ではネットワークが量子ネットワークである場合や，証明者とネットワークをなす検証者が量子対話型証明を行うような検証モデルを数理的にモデル化して，その検証能力を解明することを目指す．

３．研究の方法

本研究課題は対話型証明という計算量理論の数理モデルであるため，計算量理論および密接に関連する分野であるアルゴリズム論からの技術を基本的な道具として利用する．計算量理論，アルゴリズム論およびその量子計算版である量子計算量理論，量子アルゴリズム論は，研究代表者である西村と研究分担者であるルガル教授、森前准教授がそれぞれの知見を持ち寄ることによって，上記の目的を達成することとした．また，量子対話型証明をはじめとする量子対話プロトコルを研究するには，量子通信理論や量子情報理論の技術が不可欠であるため，量子情報理論の専門家であるブシェーミ教授を研究分担者として，必要な技術の開発や知見の展開が行われた．さらに研究の進展のために積極的に国内外の各分野の専門家からの知識提供や研究協力を仰ぐことを行った．本研究課題の 2 年目以降は COVD-19 によって国内外の研究者との対面での交流が大幅に制限されることになったが，オンライ

ンでの交流を行うことによって研究を推進した．また，3 年目途中から量子測定理論に関する知見に基づいた解析を強化するため，量子測定理論の第一人者である小澤教授を分担者として招き入れ，研究の進展を加速させた．

４．研究成果

本研究課題が行われた 4 年間で約 50 本の雑誌論文（査読付き国際会議論文を含む）を出版することができた．理論計算機科学では名の通った国際会議やハイインパクトジャーナルにも多くの論文を掲載することができて，理論の研究としては質量ともに十分な研究成果が出たと考えられる．

目的(A)に関する成果としては，合理的証明（rational proof）の概念による量子コンピュータの検証の数理モデルの提案とその研究の礎となる成果があげられる．これによって量子計算の検証に経済的な概念をはじめて導入した．その数理モデルにおいて，多項式時間量子計算に対する合理的証明プロトコルを得ることができ，量子計算の古典計算による合理的証明は可能であることを示すことができた．また，古典の対話型証明で使用される sumcheck ベースの合理的対話プロトコルを与えることにも成功した．さらには合理的証明と従来の対話型証明の間にある種の条件が成り立つときのそれらの間の計算量的等価性を与えることもできた．加えて，量子コンピュータの検証問題に関する他の方向からの研究成果も得ることができた．量子コンピュータの検証問題に対する代表的なアプローチである計算量的仮定を用いるものとしては，Brakerski らにより提案された LWE 仮定をもとにする対話型プロトコルを改良して，量子コンピュータが真に量子性を示すために必要とされる量子回路がより弱いもの（対数深さの古典回路を補助とする定数深さ量子回路）でも十分であることを示すことができた．

目的(B)に関する代表的な成果としては，2005 年に Marriott と Watrous によって提案された Arthur-Merlin ゲーム（対話型証明の一形態）の量子版を拡張して，それらによって検証可能な問題のクラスを提案した成果があげられる．この成果では，検証者の量子通信を EPR 対と呼ばれる簡素な量子もつれ状態の列に制限することで Marriott-Watrous の量子対話型証明モデルを自然な形で一般化し，そのモデルにおける量子計算量クラスを導入した．その上でそれらの量子計算量クラスに関する幾つかの計算量理論的性質を明らかにし，それらを特徴づけるような完全問題を発見した．これによって，いまだに計算量理論的解明がなされていない通信回数２回の量子対話型証明で検証可能な問題のクラスについての理解を深めることができた．また，量子もつれの対話プロトコルにおける影響を明らかにするため，量子対話型証明より簡素なモデルを新たに導入してその解析を行った．マルチパーティパーティ計算の最も簡素な形である秘密同時メッセージプロトコルについて，量子もつれの存在が通信量を削減するようなプロトコルを等価性判定や AND 関数といった重要な関数に対して構築することができた．また，通信計算量理論の枠組みにおいて，二つの離散的な確率分布が近いか否かを判定する量子通信計算プロトコルが古典の場合より二次的に通信量を削減することや，そのプロトコルが漸近的に最良であることも示すことができた．

目的(C)に関する成果としては，量子分散検証とその一般化である量子分散対話型証明があげられる．従来の分散検証では証明者が検証者であるネットワークの各ノードに入力に対して対数オーダであるような短い古典情報を証明として送り，その後のラウンドで検証

者は通信を行って入力がある条件をみたすか否かを検証する．対して，本研究課題の成果で導入した量子分散検証では，証明者からの証明も検証者同士の通信も量子に変更される．このような分散型量子プロトコルにおいて，ネットワーク上でのデータの等価性判定問題に関する効率的な量子プロトコルを構築することに成功した．この量子プロトコルは，古典の分散検証で必要とする証明の長さを指数的に改善し，分散検証における量子情報の優位性が明らかにされた．また，ネットワークの各ノードが証明者から一方向的に証明を受け取るだけでなく，対話を行える計算モデルとして量子分散対話型証明も新たに提案した．そして，任意の定数回の通信で検証可能な分散型量子対話型証明が５回の通信でも検証可能なことを示すなど，分散型量子対話型証明が持つ幾つかの基本的性質を明らかにした．また，古典の分散型対話型証明に対して優位性を持つ問題を発見した．さらには，ネットワーク上での量子通信による計算を研究する過程で量子通信計算量モデルの多人数版に関する研究も推進して，その上での通信量的限界を示すことができた．

上記の目的を推進するうえでなされた関連研究として，量子計算量理論に関する成果や量子アルゴリズムの開発，量子暗号プロトコルや量子情報理論の研究に関する成果も得られた．量子計算量理論に関する成果の代表例としては，Fine-grained complexity theory における仮定に基づき指数時間であっても古典計算機で模倣できないような量子回路を明らかにした成果がある．また，計算量的量子暗号における基本技術が何かを追跡した．古典の場合，そのような基本技術は一方向性関数であるが，一方向性関数より弱いとされる基本技術から量子ビットコミットメントや電子署名といった暗号プロトコルが導出可能であることを明らかにした．量子アルゴリズムについては，グラフ上の三角形を発見する問題や All-Pairs Shortest Path problem と呼ばれる最短路のペアを見つける問題において，古典よりも高速な量子アルゴリズムを得ることができた．また，最小スタイナー木問題に対して，現時点での最速な古典アルゴリズムよりも高速な量子アルゴリズムを新たに構築し，また，行列の特異値分解に関連する幾つかの問題について，量子アルゴリズムの概念を利用することにより，高速な古典アルゴリズムを構築することができた．量子暗号プロトコルに関する成果としては，Broadbent と Islam が 2020 年に導入した certified deletion と呼ばれる量子特有の機能を備えた様々な暗号プロトコル（公開鍵暗号や属性ベース暗号）を構築することに成功した．ゼロ知識証明の形態として新たに certified everlasting ゼロ知識というものも導入して，NP の量子版として知られる QMA 問題に対する certified everlasting ゼロ知識プロトコルを構築することに成功した．量子情報理論の成果の例としては，リソース理論における空間的に分離された様々なリソースを包含および一般化するフレームワークと，それらの非古典性を定量化するためのツールを開発することができた．また，量子アンサンブルの推測問題（guesswork）について進展を得た．一度に１つの状態しか問い合わせることができない量子アンサンブルにおいてアンサンブルの状態を正しく推測するために必要な平均推測回数の最小値を定量化して，一様な確率分布を持つ任意の量子ビットアンサンブルに対する解析解を含む有限の条件下での推測問題の解析解を導出した．さらには，量子情報理論的アプローチによる量子熱力学の導出も得た．量子誤り訂正をフィードバック制御を持つ量子熱機関として捉えて，誤り識別の段階で散逸する測定熱の上限を Groenewold 情報利得の観点から導出し，量子誤り訂正の文脈において熱力学の第二法則に関する不等式を導出した．さらにある物理仮定の下で上限が誤り訂正忠実度，熱力学的効率，誤り検出段階における量子測定の効率のトレードオフで表現できることを示した．

５．主な発表論文等

〔雑誌論文〕　計51件（うち査読付論文　49件／うち国際共著　22件／うちオープンアクセス　49件）

１．著者名 Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura, Ami Paz	４．巻 -
２．論文標題 Distributed Quantum Proofs for Replicated Data	５．発行年 2021年
３．雑誌名 Proceedings of the 12nd Innovations in Theoretical Computer Science conference (ITCS2021)	６．最初と最後の頁 28:1-28:20
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2021.28	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Dhawal Jethwani, Francois Le Gall, Sanjay K. Singh	４．巻 -
２．論文標題 Quantum-Inspired Classical Algorithms for Singular Value Transformation	５．発行年 2020年
３．雑誌名 Proceedings of the 45th International Symposium on Mathematical Foundations of Computer Science (MFCS2020)	６．最初と最後の頁 53:1-53:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.MFCS.2020.53	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Masayuki Miyamoto, Masakazu Iwamura, Koichi Kise, Francois Le Gall	４．巻 -
２．論文標題 Quantum Speedup for the Minimum Steiner Tree Problem	５．発行年 2020年
３．雑誌名 Proceedings of the 26th International Conference on Computing and Combinatorics (COCOON2020)	６．最初と最後の頁 234～245
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-58150-3_19	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Yuki Takeuchi, Tomoyuki Morimae, Seiichiro Tani	４．巻 -
２．論文標題 Sumcheck-Based Delegation of Quantum Computing to Rational Server	５．発行年 2020年
３．雑誌名 Proceedings of the 16th International Conference on Theory and Applications of Models of Computation (TAMC2020)	６．最初と最後の頁 69～81
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-59267-7_7	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名	4．巻
Michele Dall'Arno, Francesco Buscemi, Alessandro Bisio, Alessandro Tosini	102
2．論文標題	5．発行年
Data-driven inference, reconstruction, and observational completeness of quantum devices	2020年
3．雑誌名	6．最初と最後の頁
Physical Review A	62407
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1103/PhysRevA.102.062407	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	該当する

1．著者名	4．巻
Denis Rosset, David Schmid, Francesco Buscemi	125
2．論文標題	5．発行年
Type-Independent Characterization of Spacelike Separated Resources	2020年
3．雑誌名	6．最初と最後の頁
Physical Review Letters	210402
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1103/PhysRevLett.125.210402	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	該当する

1．著者名	4．巻
Wenbin Zhou, Francesco Buscemi	53
2．論文標題	5．発行年
General state transitions with exact resource morphisms: a unified resource-theoretic approach	2020年
3．雑誌名	6．最初と最後の頁
Journal of Physics A: Mathematical and Theoretical	445303-445303
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1088/1751-8121/abafe5	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名	4．巻
Francesco Buscemi, Daichi Fujiwara, Naoki Mitsui, Marcello Rotondo	102
2．論文標題	5．発行年
Thermodynamic reverse bounds for general open quantum processes	2020年
3．雑誌名	6．最初と最後の頁
Physical Review A	32210
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1103/PhysRevA.102.032210	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名 Yi-Zheng Zhen, Yingqiu Mao, Kai Chen, Francesco Buscemi, Oscar Dahlsten	4．巻 101
2．論文標題 Unified approach to witness non-entanglement-breaking quantum channels	5．発行年 2020年
3．雑誌名 Physical Review A	6．最初と最後の頁 62301
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.101.062301	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Hirotada Kobayashi, Francois Le Gall, Harumichi Nishimura	4．巻 48
2．論文標題 Generalized Quantum Arthur-Merlin Games	5．発行年 2019年
3．雑誌名 SIAM Journal on Computing	6．最初と最後の頁 865～902
掲載論文のDOI（デジタルオブジェクト識別子） 10.1137/17M1160173	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 西村治道	4．巻 48(2)
2．論文標題 或る理論計算機科学の研究者から見た量子コンピュータの歴史	5．発行年 2020年
3．雑誌名 現代思想	6．最初と最後の頁 54～64
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Francesco Buscemi, Eric Chitambar, Wenbin Zhou	4．巻 124
2．論文標題 Complete Resource Theory of Quantum Incompatibility as Quantum Programmability	5．発行年 2020年
3．雑誌名 Physical Review Letters	6．最初と最後の頁 120401
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevLett.124.120401	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Michele Dall'Arno, Francesco Buscemi, Valerio Scarani	4．巻 4
2．論文標題 Extension of the Alberti-Ulhmann criterion beyond qubit dichotomies	5．発行年 2020年
3．雑誌名 Quantum	6．最初と最後の頁 233
掲載論文のDOI（デジタルオブジェクト識別子） 10.22331/q-2020-02-20-233	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Bartosz Regula, Varun Narasimhachar, Francesco Buscemi, Mile Gu	4．巻 2
2．論文標題 Coherence manipulation with dephasing-covariant operations	5．発行年 2020年
3．雑誌名 Physical Review Research	6．最初と最後の頁 13109
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevResearch.2.013109	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francesco Buscemi, David Sutter, Marco Tomamichel	4．巻 3
2．論文標題 An information-theoretic treatment of quantum dichotomies	5．発行年 2019年
3．雑誌名 Quantum	6．最初と最後の頁 209
掲載論文のDOI（デジタルオブジェクト識別子） 10.22331/q-2019-12-09-209	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francesco Buscemi, Michele Dall'Arno	4．巻 21
2．論文標題 Data-driven inference of physical devices: theory and implementation	5．発行年 2019年
3．雑誌名 New Journal of Physics	6．最初と最後の頁 113029
掲載論文のDOI（デジタルオブジェクト識別子） 10.1088/1367-2630/ab5003	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Iris Agresti, Davide Poderini, Gonzalo Carvacho, Leopoldo Sarra, Rafael Chaves, Francesco Buscemi, Michele Dall'Arno, Fabio Sciarrino	4．巻 4
2．論文標題 Experimental semi-device-independent tests of quantum channels	5．発行年 2019年
3．雑誌名 Quantum Science and Technology	6．最初と最後の頁 35004
掲載論文のDOI（デジタルオブジェクト識別子） 10.1088/2058-9565/ab19f2	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Tomoyuki Morimae, Suguru Tamaki	4．巻 19
2．論文標題 Fine-grained quantum computational supremacy	5．発行年 2019年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 1089～1115
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC19.13-14-2	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Tomoyuki Morimae, Harumichi Nishimura, Yuki Takeuchi, Seiichiro Tani	4．巻 19
2．論文標題 Impossibility of blind quantum sampling for classical client	5．発行年 2019年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 793～806
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC19.9-10-3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Yuki Takeuchi, Tomoyuki Morimae, Masahito Hayashi	4．巻 9
2．論文標題 Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements	5．発行年 2019年
3．雑誌名 Scientific Reports	6．最初と最後の頁 13585
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41598-019-49968-3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Yuki Takeuchi, Atul Mantri, Tomoyuki Morimae, Akihiro Mizutani, Joseph F. Fitzsimons	4．巻 5
2．論文標題 Resource-efficient verification of quantum computing using Serfling’s bound	5．発行年 2019年
3．雑誌名 npj Quantum Information	6．最初と最後の頁 27
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41534-019-0142-2	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Tomoyuki Morimae, Harumichi Nishimura	4．巻 20
2．論文標題 Rational proofs for quantum computing	5．発行年 2020年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 181～193
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC20.3-4-1	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Taisuke Izumi, Francois Le Gall, Frederic Magniez	4．巻 -
2．論文標題 Quantum Distributed Algorithm for Triangle Finding in the CONGEST Model	5．発行年 2020年
3．雑誌名 Proceedings of the 37th International Symposium on Theoretical Aspects of Computer Science (STACS2020)	6．最初と最後の頁 23:1～23:13
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.STACS.2020.23	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francois Le Gall	4．巻 -
2．論文標題 Average-Case Quantum Advantage with Shallow Circuits	5．発行年 2019年
3．雑誌名 Proceedings of the 34th Computational Complexity Conference (CCC2019)	6．最初と最後の頁 21:1～21:20
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.CCC.2019.21	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Taisuke Izumi, Francois Le Gall	4．巻 -
2．論文標題 Quantum Distributed Algorithm for the All-Pairs Shortest Path Problem in the CONGEST-CLIQUE Model	5．発行年 2019年
3．雑誌名 Proceeding of the 38th ACM Symposium on Principles of Distributed Computing (PODC2019)	6．最初と最後の頁 84～93
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3293611.3331628	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Keren Censor-Hillel, Orr Fischer, Francois Le Gall, Dean Leitersdorf, Rotem Oshman	4．巻 -
2．論文標題 Quantum Distributed Algorithms for Detection of Cliques	5．発行年 2022年
3．雑誌名 Proceedings of the 13th Innovations in Theoretical Computer Science conference (ITCS2022)	6．最初と最後の頁 35:1-35:25
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2022.35	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francois Le Gall, Saeed Seddighin	4．巻 -
2．論文標題 Quantum Meets Fine-grained Complexity: Sublinear Time Quantum Algorithms for String Problems	5．発行年 2022年
3．雑誌名 Proceedings of the 13th Innovations in Theoretical Computer Science conference (ITCS2022)	6．最初と最後の頁 97:1-97:23
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2022.97	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Aleksandrs Belovs, Arturo Castellanos, Francois Le Gall, Guillaume Malod, Alexander A. Sherstov	4．巻 21
2．論文標題 Quantum communication complexity of distribution testing	5．発行年 2021年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 1261～1273
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC21.15-16-1	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francois Le Gall, Masayuki Miyamoto	4．巻 -
2．論文標題 Lower Bounds for Induced Cycle Detection in Distributed Computing	5．発行年 2021年
3．雑誌名 Proceedings of the 32nd International Symposium on Algorithms and Computation (ISAAC2021)	6．最初と最後の頁 58:1-58:19
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ISAAC.2021.58	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Francois Le Gall, Atsuya Hasegawa	4．巻 -
2．論文標題 Quantum Advantage with Shallow Circuits under Arbitrary Corruption	5．発行年 2021年
3．雑誌名 Proceedings of the 32nd International Symposium on Algorithms and Computation (ISAAC2021)	6．最初と最後の頁 74:1-74:16
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ISAAC.2021.74	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Shuichi Hirahara, Francois Le Gall	4．巻 -
2．論文標題 Test of Quantumness with Small-Depth Quantum Circuits	5．発行年 2021年
3．雑誌名 Proceedings of the 46th International Symposium on Mathematical Foundations of Computer Science (MFCS2021)	6．最初と最後の頁 59:1-59:15
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.MFCS.2021.59	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Francois Le Gall, Harumichi Nishimura, Abuzer Yakaryilmaz	4．巻 -
2．論文標題 Quantum Logarithmic Space and Post-selection	5．発行年 2021年
3．雑誌名 Proceedings of the 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC2021)	6．最初と最後の頁 10:1-10:17
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.TQC.2021.10	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Akinori Kawachi, Harumichi Nishimura	4．巻 -
2．論文標題 Communication Complexity of Private Simultaneous Quantum Messages Protocols	5．発行年 2021年
3．雑誌名 Proceedings of the 2nd Conference on Information-Theoretic Cryptography (ITC2021)	6．最初と最後の頁 20:1-20:19
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITC.2021.20	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Michele Dall'Arno, Sarah Brandsen, Francesco Buscemi	4．巻 27
2．論文標題 Explicit Construction of Optimal Witnesses for Input-Output Correlations Attainable by Quantum Channels	5．発行年 2020年
3．雑誌名 Open Systems and Information Dynamics	6．最初と最後の頁 2050017
掲載論文のDOI（デジタルオブジェクト識別子） 10.1142/S1230161220500171	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francesco Buscemi, Valerio Scarani	4．巻 103
2．論文標題 Fluctuation theorems from Bayesian retrodiction	5．発行年 2021年
3．雑誌名 Physical Review E	6．最初と最後の頁 52111
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevE.103.052111	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Clive Cenxin Aw, Francesco Buscemi, Valerio Scarani	4．巻 3
2．論文標題 Fluctuation theorems with retrodiction rather than reverse processes	5．発行年 2021年
3．雑誌名 AVS Quantum Science	6．最初と最後の頁 45601
掲載論文のDOI（デジタルオブジェクト識別子） 10.1116/5.0060893	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Michele Dall'Arno, Francesco Buscemi, Takeshi Koshiba	4．巻 68
2．論文標題 Guesswork of a Quantum Ensemble	5．発行年 2022年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 3139～3143
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2022.3146463	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, Takashi Yamakawa	4．巻 1
2．論文標題 Quantum Encryption with Certified Deletion, Revisited: Public Key, Attribute-Based, and Classical Communication	5．発行年 2021年
3．雑誌名 Proceedings of the 27th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT2021)	6．最初と最後の頁 606～636
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92062-3_21	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 西村治道	4．巻 61
2．論文標題 量子回路の計算複雑性について	5．発行年 2022年
3．雑誌名 数学セミナー	6．最初と最後の頁 26-31
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Masanao Ozawa, Andrei Khrennikov	4．巻 112
2．論文標題 Nondistributivity of human logic and violation of response replicability effect in cognitive psychology	5．発行年 2023年
3．雑誌名 Journal of Mathematical Psychology	6．最初と最後の頁 102739
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jmp.2022.102739	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Shintaro Minagawa, Hayato Arai, Francesco Buscemi	4．巻 4
2．論文標題 Von Neumann's information engine without the spectral theorem	5．発行年 2022年
3．雑誌名 Physical Review Research	6．最初と最後の頁 33091
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevResearch.4.033091	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Arshag Danageozian, Mark M. Wilde, Francesco Buscemi	4．巻 3
2．論文標題 Thermodynamic Constraints on Quantum Information Gain and Error Correction: A Triple Trade-Off	5．発行年 2022年
3．雑誌名 PRX Quantum	6．最初と最後の頁 20318
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PRXQuantum.3.020318	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Tomoyuki Morimae, Takashi Yamakawa	4．巻 4
2．論文標題 Classically Verifiable NIZK for QMA with Preprocessing	5．発行年 2022年
3．雑誌名 Proceedings of the 28th International Conference on the Theory and Application of Cryptology and Information Security (ASIacrypt2022)	6．最初と最後の頁 599～627
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-22972-5_21	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, Takashi Yamakawa	4．巻 1
2．論文標題 Certified Everlasting Zero-Knowledge Proof for QMA	5．発行年 2022年
3．雑誌名 Proceedings of the 42nd Annual International Cryptology Conference (CRYPTO2022)	6．最初と最後の頁 239～268
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15802-5_9	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Tomoyuki Morimae, Takashi Yamakawa	4．巻 1
2．論文標題 Quantum Commitments and Signatures Without One-Way Functions	5．発行年 2022年
3．雑誌名 Proceedings of the 42nd Annual International Cryptology Conference (CRYPTO2022)	6．最初と最後の頁 269～295
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15802-5_10	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Tomoyuki Morimae, Takashi Yamakawa	4．巻 -
2．論文標題 Proofs of Quantumness from Trapdoor Permutations	5．発行年 2023年
3．雑誌名 Proceedings of the 14th Innovations in Theoretical Computer Science conference (ITCS2023)	6．最初と最後の頁 87:1-87:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2023.87	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Sevag Gharibian, Francois Le Gall	4．巻 -
2．論文標題 Dequantizing the Quantum Singular Value Transformation: Hardness and Applications to Quantum Chemistry and the Quantum PCP Conjecture	5．発行年 2022年
3．雑誌名 Proceedings of the 54th ACM Symposium on Theory of Computing (STOC2022)	6．最初と最後の頁 19-32
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3519935.3519991	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Francois Le Gall, Daiki Suruga	4．巻 -
2．論文標題 Bounds on Oblivious Multiparty Quantum Communication Complexity	5．発行年 2022年
3．雑誌名 Proceedings of the 15th Lation American Theoretical Informatics Symposium (LATIN2022)	6．最初と最後の頁 641～657
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20624-5_39	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Francois Le Gall, Iu-iong Ng	4．巻 22
2．論文標題 Quantum approximate counting for Markov chains and collision counting	5．発行年 2022年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 1261～1279
掲載論文のDOI（デジタルオブジェクト識別子） 10.26421/QIC22.15-16-1	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Atsuya Hasegawa, Francois Le Gall	4．巻 -
2．論文標題 An optimal oracle separation of classical and quantum hybrid schemes	5．発行年 2022年
3．雑誌名 Proceedings of the 33rd International Symposium on Algorithms and Computation (ISAAC2022)	6．最初と最後の頁 6:1-6:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ISAAC.2022.6	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Francois Le Gall, Masayuki Miyamoto, Harumichi Nishimura	4．巻 -
2．論文標題 Distributed Quantum Interactive Proofs	5．発行年 2023年
3．雑誌名 Proceedings of the 40th International Symposium on Theoretical Aspects of Computer Science (STACS2023)	6．最初と最後の頁 42:1-42:21
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.STACS.2023.42	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計39件（うち招待講演　22件／うち国際学会　32件）

1．発表者名 Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura, Ami Paz
2．発表標題 Brief Announcement: Distributed Quantum Proofs for Replicated Data
3．学会等名 34th International Symposium on Distributed Computing（国際学会）
4．発表年 2020年

１．発表者名
Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura, Ami Paz

２．発表標題
Distributed Quantum Proofs for Replicated Data

３．学会等名
24th Workshop on Quantum Information Processing（国際学会）

４．発表年
2021年

１．発表者名
Harumichi Nishimura

２．発表標題
SWAP Test and Its Applications to Quantum Distributed Computing

３．学会等名
2nd Workshop on Quantum and Classical Cryogenic Devices, Circuits, and Systems（国際学会）

４．発表年
2020年

１．発表者名
Francois Le Gall

２．発表標題
Average-case Quantum Advantage with Shallow Circuits

３．学会等名
2nd Workshop on Quantum and Classical Cryogenic Devices, Circuits, and Systems（国際学会）

４．発表年
2020年

１．発表者名
Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura, Ami Paz

２．発表標題
Distributed Quantum Proofs for Replicated Data

３．学会等名
第1回量子ソフトウェア研究会

４．発表年
2020年

１．発表者名
Francesco Buscemi

２．発表標題
Using data-driven inference to bootstrap quantum tomography

３．学会等名
2nd workshop on Quantum and Classical Cryogenic Devices, Circuits, and Systems（国際学会）

４．発表年
2020年

１．発表者名
Francesco Buscemi

２．発表標題
Statistical tests of "quantumness": from mathematics to technology

３．学会等名
20th Asian Quantum Information Science Conference（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
Francesco Buscemi

２．発表標題
Optimal hiding/masking of quantum information

３．学会等名
Online Workshop on Quantum Information, Computation, and Foundations（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
Harumichi Nishimura

２．発表標題
Possibility of classical verification for quantum computation

３．学会等名
Nagoya-SUSTech Quantum Information Workshop（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Harumichi Nishimura

２．発表標題
Classical verification for quantum computation

３．学会等名
Workshop on Quantum Protocol（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Harumichi Nishimura

２．発表標題
More approaches for studying classical verification of quantum computation

３．学会等名
1st Workshop on Quantum and Classical Cryogenic Devices, Circuits, and Systems (QCCC2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
森前智行，西村治道

２．発表標題
Rational proofs for quantum computing

３．学会等名
コンピュテーション研究会

４．発表年
2019年

１．発表者名
Francesco Buscemi

２．発表標題
Data-Driven Inference and Observationally Complete Devices

３．学会等名
12th Italian Quantum Information Science Conference（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Francesco Buscemi

２．発表標題
Statistical Comparison and Its Applications in Quantum Information Theory

３．学会等名
4th Workshop on Mathematical Physics and Quantum Information Theory（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Francesco Buscemi

２．発表標題
Data-Driven Inference and Observationally Complete Devices

３．学会等名
51th Symposium in Mathematical Physics（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Francesco Buscemi

２．発表標題
Data-Driven Inference and Observationally Complete Devices

３．学会等名
Quantum Information Revolution: Impact to Foundations（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Francesco Buscemi

２．発表標題
Quantum Statistical Comparison, Quantum Majorization, and Their Applications to Generalized Resource Theories

３．学会等名
Mathematical Aspects in Current Quantum Information Theory (MAQIT)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Francesco Buscemi

２．発表標題
"Semiquantum games" to verify quantum correlations (in space and time)

３．学会等名
Nagoya-SUSTech Quantum Information Workshop（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Taisuke Izumi, Francois Le Gall, Frederic Magniez

２．発表標題
Quantum Distributed Algorithm for Triangle Finding in the CONGEST Model

３．学会等名
37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)（国際学会）

４．発表年
2020年

１．発表者名
Francois Le Gall

２．発表標題
Average-Case Quantum Advantage with Shallow Circuits

３．学会等名
34th Computational Complexity Conference (CCC 2019)（国際学会）

４．発表年
2019年

１．発表者名
Taisuke Izumi, Francois Le Gall

２．発表標題
Quantum Distributed Algorithm for the All-Pairs Shortest Path Problem in the CONGEST-CLIQUE Model

３．学会等名
2019 ACM Symposium on Principles of Distributed Computing (PODC 2019)（国際学会）

４．発表年
2019年

１．発表者名
Francois Le Gall

２．発表標題
Quantum algorithms for large-scale problems

３．学会等名
Quantum Innovation 2021, the International Symposium on Quantum Science, Technology and Innovation（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Francois Le Gall, 宮本昌幸

２．発表標題
分散計算における誘導サイクル発見問題の下界

３．学会等名
電子情報通信学会コンピュテーション研究会

４．発表年
2021年

１．発表者名
Francesco Buscemi

２．発表標題
The "thermodynamic reverse bound" and the role of retrodiction in the Second law

３．学会等名
SUSTech-Nagoya workshop on Quantum Science（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Francesco Buscemi

２．発表標題
Prediction, retrodiction, and the Second Law of Thermodynamics

３．学会等名
Summer School on Quantum Information and Quantum Technology（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Francesco Buscemi

２．発表標題
The Petz map in maths, information theory, and physics: an overview

３．学会等名
Workshop on Quantum Information and Quantum Black Holes（招待講演）

４．発表年
2021年

１．発表者名
Francesco Buscemi

２．発表標題
Bayesian Retrodiction and the Second Law of Thermodynamics

３．学会等名
Second Kyoto Workshop on Quantum Information, Computation, and Foundation（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Harumichi Nishimura

２．発表標題
SMP model, PSM protocols, and their quantum analogues

３．学会等名
SUSTech-Nagoya workshop on Quantum Science（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Harumichi Nishimura

２．発表標題
Simultaneous Message Passing Models and Private Simultaneous Message Protocols with Shared Entanglement

３．学会等名
3rd Workshop on Quantum and Classical Cryogenic Devices, Circuits, and Systems (QCCC2021)（国際学会）

４．発表年
2021年

１．発表者名
武田玲志，西村治道

２．発表標題
AND関数に対する秘密同時メッセージプロトコル

３．学会等名
第45回量子情報技術研究会

４．発表年
2021年

１．発表者名
川合達也，西村治道

２．発表標題
群非同型性判定問題の証拠生成に対する検証プロトコル

３．学会等名
第8回量子ソフトウェア研究会

４．発表年
2023年

１．発表者名
Harumichi Nishimura

２．発表標題
Power of Distributed Quantum Merlin-Arthur Proofs

３．学会等名
SUS-Tech-Nagoya Workshop on Quantum Science（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
小澤正直

２．発表標題
量子測定とは何を測定するのか：測定誤差の定義と測定値の観測者独立性

３．学会等名
九大IMI共同利用研究会「時間・量子測定・準古典近似の理論と実験」（招待講演）

４．発表年
2022年

１．発表者名
Masanao Ozawa

２．発表標題
Logical Characterication of Contextual Hidden-Variable Theories based on Quantum Set Theory

３．学会等名
19th International Conference on Quantum Physics and Logic (QPL2022)（国際学会）

４．発表年
2022年

１．発表者名
Haruki Emori, Masanao Ozawa, Akihisa Tomita

２．発表標題
Disturbance Evaluation Circuit in Quantum Measurement

３．学会等名
Asian Conference on Quantum Information Science 2022 (AQIS2022)（国際学会）

４．発表年
2022年

１．発表者名
Francesco Buscemi

２．発表標題
Fluctuation relations and the second law of thermodynamics from Bayesian retrodiction

３．学会等名
Quantum Information and Probability: from Foundations to Engineering（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Francesco Buscemi

２．発表標題
The theory of statistical comparison: a brief overview

３．学会等名
SUSTech-Nagoya Workshop on Quantum Science（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Francois Le Gall

２．発表標題
Quantum Distributed Computing

３．学会等名
Workshop on Advances in Distributed Graph Algorithms (ADGA2022)（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Sevag Gharibian, Ryu Hayakawa, Francois Le Gall, Tomoyuki Morimae

２．発表標題
Improved Hardness Results for the Guided Local Hamiltonian Problem

３．学会等名
26th Conference on Quantum Information Processing (QIP2023)（国際学会）

４．発表年
2023年

〔図書〕　計1件

１．著者名 西村 治道	４．発行年 2022年
２．出版社 オーム社	５．総ページ数 264
３．書名 基礎から学ぶ量子計算	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	ルガル　フランソワ (Le Gall Francois) (50584299)	名古屋大学・多元数理科学研究科・教授 (13901)	

6．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	森前　智行 (Morimae Tomoyuki) (50708302)	京都大学・基礎物理学研究所・准教授 (14301)	
研究分担者	Ｂｕｓｃｅｍｉ　Ｆ. (Buscemi Francesco) (80570548)	名古屋大学・情報学研究科・教授 (13901)	
研究分担者	小澤　正直 (Ozawa Masanao) (40126313)	中部大学・AI数理データサイエンスセンター・特任教授 (33910)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
フランス	CNRS	Universite de Paris		
オーストリア	Universitat Wien			
中国	Southern Univ. Science and Technology	Univ. Science and Technology of China		
インド	Indian Institutes of Technology			
カナダ	Perimeter Institute			
シンガポール	National University of Singapole			
イスラエル	Technion	Tel-Aviv University		
ラトビア	University of Latvia			
米国	Toyota Tech. Institute at Chicago	University of California	Duke University	他1機関
ドイツ	Paderborn University			

共同研究相手国	相手方研究機関			
スウェーデン	Linnaeus Unniversity			