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　４ 年　 ６ 月 １６ 日現在

機関番号：３２６８９
研究種目：基盤研究(A)（一般）
研究期間：2016～2020
課題番号：１６Ｈ０１７０５

研究課題名（和文）量子プロトコル理論の線的展開

研究課題名（英文）Interpolative Expansion of Quantum Protocol Theory

研究代表者
小柴　健史（Takeshi, Koshiba）

早稲田大学・教育・総合科学学術院・教授

研究者番号：６０４００８００

交付決定額（研究期間全体）：（直接経費）　　32,100,000円

研究成果の概要（和文）：量子状態の初期化が容易でない量子計算を定式化したDQC1モデルなどの計算能力を究明することにより，万能でない量子計算モデルでさえ量子超越性を達成し得ることを示した。量子分散アルゴリズムに関しては，標準的な分散計算モデルにおいて「全対最短経路問題」などの幾つかの基本的問題について，古典プロトコルよりも効率的に動作する量子分散プロトコルを開発した。量子暗号プロトコルである秘匿代理量子計算において，古典クライアントでは，完全秘匿性を達成不可能であることを示した。量子性の古典的検証可能性に，報酬概念を導入することで，ゲーム理論的な形での解決という新しい方向性を見出した。

研究成果の学術的意義や社会的意義
従来の量子アルゴリズムの研究は，古典的手法に対して量子的手法の優勢性を示すことが中心であった。本研究課題においては，汎用量子コンピュータより早期の実現可能性が高い計算モデルにおける量子超越性を示し，量子分散アルゴリズムという分野を新たに開拓し世界をリードする存在であり，量子計算という研究領域を拡大させている。その意味で学術的に大きく貢献していると考えられる。また，非万能量子計算や量子分散アルゴリズムにおける量子計算は比較的小規模であり，量子計算研究の現実的側面を強調するという意義もある。

研究成果の概要（英文）：The computational power of the DQC1 model, which is a formalization of non-universal quantum computation with initialization-hard quantum states, is shown to be superior to classical computation. Many quantum distributed algorithms are developed. Under the standard model for distributed algorithms, efficient quantum protocols for several fundamental problems such as the shortest path problem. Secure quantum delegated computation cannot achieve the perfect security for classical clients. By introducing the notion of rewards in quantum computations, classical verification of having the quantum power of the server is affirmatively settled. This is a game-theoretic solution and gives a novel method in quantum computation.

研究分野：量子情報学

キーワード：量子計算　量子アルゴリズム　量子プロトコル　量子通信　計算量理論　暗号理論　分散アルゴリズム　量子暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

量子情報科学は，量子力学に基づいた計算・通信モデルを考えることにより，従来の情報科学の限界を超えた強力な情報処理を可能にする分野として注目され発展してきている。例えば，Bennett & Brassard による BB84 プロトコルは二者間通信における無条件に安全な鍵共有法を与える。また Broadbent,Fitzsimons & Kashefi は万能ブラインド計算(Proc.FOCS2009,pp.517-526)と呼ばれる無条件に安全な代理計算プロトコルを構築している。前身研究課題「量子プロトコル理論の深化」においても，申請者らは，量子情報理論と量子計算量理論双方の知見を組み合わせ，多くの量子プロトコルの設計に寄与してきた。その研究目的のため量子プロトコルの可能性追究を深さ優先で行ってきた結果でもある。

近年，量子情報科学に対する見方も変化しつつある。例えば，NSA(アメリカ国家安全保障局)は，暗号開発ベンダーに対して量子コンピュータに対する攻撃を想定するように促す声明を発表しているように，量子コンピュータを直近の脅威として認識している。さらに，大規模データに対する情報処理技術が進むと同時にプライバシーの問題も複雑化してきている。Google が支援する 23andMe など，人の遺伝子情報解析を数日で行い，それをもとにしたオーダーメード創薬も実現目前のものとなっている。特に，遺伝子情報は子孫にも継承されるため，ロングスパンでの高い安全性が要求される。そのため，将来出現する量子コンピュータに対する安全性も考慮することが望ましい。

現在実際に利用されている情報セキュリティ技術は量子コンピュータに対して脆弱であるが，量子コンピュータが実現したとしても，量子コンピュータに対する解法が知られていない格子問題や符号理論に基づく暗号プロトコルに置換することで当面の対策は可能である。また，暗号プロトコルは単体で安全な方式を組み合わせて利用したときには安全性が保証されないことが知られているが，それを保証する性質として汎用結合可能性と呼ばれている強い安全性概念がある。Unruh(Proc.EUROCRYPT2010,pp.486-505)により情報理論的汎用結合可能性を持つ暗号プロトコルは量子情報理論的汎用結合可能性をもつことが示されており，現在技術で十分に強力な安全性概念を達成している方式については，量子コンピュータに対して安全であることも分かっている。その一方で，広範に量子情報技術を利用する様々な技術(例えば，研究代表者らの量子公開鍵暗号)が開発されている。今までは，量子コンピュータの実現が現実的であると捉えられていなかったこともあり，量子情報技術と通常の情報処理技術を融合するハイブリッド方式は研究されてこなかったと言える。

暗号理論の枠組みにおいては，共通鍵暗号方式と公開鍵暗号方式があるが用途も異なりそれぞれ発展してきている。両者のハイブリッド方式を導入することにより，KEM/DEM フレームワークと呼ばれる公開鍵暗号方式の設計方法に新たな指針を与えたとともに公開鍵暗号の安全性の本質を追究するためのきっかけをも与えた。ハイブリッド方式は 2 者の長所をうまく活かすだけでなく，従来無かった視点を与えることができる好例でもある。

２．研究の目的

量子情報科学は，情報科学において量子力学的な状態やその操作が可能であるとき，従来の情報科学の限界を超えることができ，その可能性を究明することを目的に発展してきている。しかしながら，従来の研究は量子情報科学に優位がある問題を個別に発見することに主眼が置かれている側面がある。本研究課題においては，現在から量子情報処理が十分に発展する未来に亘って存在する諸問題に対して，技術の発展を考慮した連続的な解決方法を提供する手段として通常の情報科学と量子情報科学の両者に基づくハイブリッドな方法論を構築することを目的とする。特に，長期に亘ってプライバシーを保護する必要な課題に対して連続的な解決方法を提供することを目指す。

３．研究の方法

研究を円滑かつ集中的に行うため 3 つのアプローチを導入しアプローチ毎の班体制を取る。班構成として，量子計算緩和班・ハイブリッド構成班・新理論援用班を導入するが，班の間の連携を密にするため，毎年，研究会を実施するとともに，他の班のプロジェクトに対して研究の方向性を議論する打合せを行い，各プロジェクトを有機的に機能させ，量子プロトコル理論の線的展開を図るべく調整を行う。また，班員編成は固定させずにトピックに応じて変化させることで，流動性を確保するとともに共通目的意識の維持を図る。研究遂行上の共有必要に応じて，海外から関連分野の研究者を招聘し研究討論する。

【研究体制】

研究体制は，量子計算緩和班(A 班)，ハイブリッド構成(B 班)，新理論援用班(C 班)で構成する。A 班は，従来型の量子プロトコルに対して利用する量子資源を限定する計算モデルを導入するという意味でトップダウン型であり，量子情報理論と量子計算量理論の両者に精通している者を中心とする。B 班は，古典安全と量子安全なハイブリッドな構成を持つプロトコルを構成するという意味でボトムアップ型であり，古典プロトコルに造詣の深い者を中心とする。C

班は，既存の枠に捉 われず量子プロトコル理論の新しい展開を目指し，A 班および B 班に知見をもたらす役割を果たしてもらう。ゲーム理論や情報の複雑さ理論(Information Complexity)に習熟している者を中心とする。また，A 班と B 班は互いに関連しており得られた知見を相互フィードバックしながら研究を遂行する。

アプローチ(A):量子計算能力を限界した計算モデルでの量子プロトコルの理論と設計方法
対話型証明はプロトコル理論における王道的トピックであり，量子対話型証明の可能性を追究する。前身研究で提案された一般化量子 Arthur-Merlin 証明(研究業績[8])の計算構□とその応用，とりわけ成果として得られた Babai の崩壊定理の量子版の応用を探究することにより，1 ラウンド量子型証明で可能なことやその限界を解明することを目指す。また，初期化された量子ビット数が極端に少ない状況など，使える量子資源が限られた状況下における量子計算モデルを検討し，その基本的性質や古典計算との差異，通常の量子計算モデルとの比較などを行うことで，現在でも実現可能なレベルの量子情報技術における量子計算の計算能力に対する理解を深める。

アプローチ(B):量子計算に対して安全な古典プロトコルの理論と設計方法
このアプローチではハイブリッド結合時の情報漏洩とシステム階層化をする際の基準(例えばプライバシーと計算量のトレードオフ)作成を，量子プロトコル理論の線的展開を考えるための要素技術と考え，初年度はこの 2 テーマに注力する。古典的な暗号プロコトルにおいて，暗号文復号や署名生成に用いられる秘密鍵情報や乱数情報が，漏洩する可能性が指摘されている。暗号プロトコルを実際に利用する際には，これら漏洩をどのように防止するか，あるいは漏洩がある範囲で起きた場合でのシステム全体の安全性に影響を及ぼす影響について理解を深める。量子コンピュータが一般利用できる時代におけるプロトコル，また，つなぎの技術としてのプロトコル，どちらにおいても，量子計算機，古典計算機の組み合わせでプロトコルが実装されると予想される。さらに，異なる計算機をつなぎ合わせ，量子チャネルや古典チャネルへのつなぎ合わせの形での利用が予想される。このつなぎ合わせで問題となるのは，つなぎ合わせにおける漏洩の防止や漏洩への耐性である。古典的な計算モデルにおける情報漏洩に加え，量子計算モデルにおける情報漏洩，二つの計算モデルにおける情報漏洩の組み合わせなどが研究対象となる。古典的な計算モデルの一つであるスプリットステートモデルを拡張し，古典的な計算モデルと量子計算モデルを積極的に分けて用いるモデルの可能性について究明を図る。
　プライバシーの長期的な安全性を保証するためには，基盤となる計算困難問題の計算量理論的な計算困難性解析に加え，その計算困難性とプライバシーの関係の精密な解析が重要となる。この関係は帰着(ある問題が計算困難であればプライバシーが保護される)という形で与えられ，関係が緊密である，つまり効率的に帰着可能であるほど基盤となる問題の計算困難性に近いプライバシーが得られることになる。したがって問題とプライバシーの帰着によるより効率の良い関係付けとその限界を研究することはプライバシーを保護できる期間を見極めるために非常に重要であり，初年度では前述の研究動機から古典・量子通信の両面から現在知られている有用な帰着技術を観察し，長期プライバシー保護に向けて新たな帰着技術の開発及びその技術によるシステ ムの設計・理論的解析を目指す。

アプローチ(C):新たなフレームワークによる量子プロトコルの可能性の追究
このアプローチでは，ゲーム理論および情報の複雑さの理論(Information Complexity)に着目して，量子プロトコル理論の線的展開へ適応させることを考える。暗号プロトコル利用者の長期的な関係性を考慮すると，ゲーム理論に基づいた安全性に繰り返
しゲームの仕組みを導入することが望ましいと考え，プロトコルを効率的に実行する方法論を構築することを目指す。特に，均衡概念や利得関数の柔軟な設計により，様々な強度の安全性が必 要な階層的システムに対して適切な安全性を提供する方法を構築する。秘密分散の復元を繰り返しゲームとみなした研究は Maleka，Shareef & Rangan (Proc.IPSEC 2008，pp.334-346)などで行われているが，その他の要素プロトコルへ拡張した研究はなく，計算量を制限したプレイヤーに対する繰り返しゲームの近似均衡解に関する研究は Halpern，Pass，Seeman (Proc. WINE2014，pp.249-262)で行われているが、具体的な暗号プロトコルに対する議論は行われていない。初年度は，紛失通信やコミットメント，秘密分散法などの重要な要素プロトコルの実現を目指す。
　古典通信において，プロトコル解析とプライバシー保証をするために重要な概念として情報の複雑さが存在している。近年，量子情報の複雑さは量子プロトコルの解明に対して有用なツールとして利用され始めているものの，古典情報の複雑さの概念のようには十分その性質が究明されていない。量子情報の複雑さの場合，定義が定まっておらず，予備的な結果として既存の定義間の関係を得ており(国際会議 AQIS2015 にて既発表)，これを用いて量子情報の複雑さの理論を整備応用することを目指す。まずは単純な場合として 2 者間の量子プロトコル間の通信の複雑さとの関係を明確にする。

【初期役割分担および遂行困難時対応】
(研究進捗状況に応じた役割分担の変更は随時行う)

担当者	主な役割	担当者	主な役割
小柴	A 班:観測ベース量子計算, B 班:同種写像, 研究総括	河内	B 班: 計算困難性とプライバシー帰着, 計算量理論に関する支援
松本	A 班:量子対話型証明, 量子情報理論に関する支援	西村	A 班:量子計算量理論
小林	A 班:量子対話型証明	ルガル	C 班:量子情報複雑性, 量子アルゴリズムに関する支援
田中	B 班:耐量子攻撃安全暗号	安永	C 班:ゲーム理論的暗号理論, 符号理論に関する支援

担当者の班内での主たる役割は上の表に記載の通りであるが，各自が得意とする専門分野もあり，その点も併記した。研究計画が計画通り進まない場合の対策として，以下の研究協力者の技術的支援を仰ぐことにより，円滑な遂行を目指す。

- Richard Cleve (Univ. Waterloo, Canada)，専門:量子対話型証明など
- Iordanis Kerenidis (Univ. Paris Diderot, France)，専門:量子プロトコルに関する限界
- 林正人(名古屋大学)，専門:量子情報理論
- 森前智行(群馬大学)，専門:観測ベース量子計算

４．研究成果

(1) 万能でない量子計算モデルの研究

DQC1 モデルは量子状態の初期化が容易でない量子計算を定式化した量子計算モデルであり，DQC1 モデルの計算誤りを低減化する方法を新たに提案した。この手法を用いて DQC1 モデルの古典計算による摸倣不可能性を示唆する計算量的帰結を与え，DQC1 モデルは量子計算モデルとしては比較的弱いモデルでありながらも古典計算ではできないことを行える証拠を得た。また，DQC1 モデルの古典計算による摸倣不可能性を追究し，理想的状況では純粋状態にあるたった１つの量子ビットすら誤りを含むような状況でもその程度によってはその出力分布が古典的に模倣可能でないような場合があることを示した。万能でない量子計算機でさえ古典計算機に対して優位であることを表す量子超越性について，DQC1 モデル及び HC1Q という新しい量子計算モデルの量子超越性を示した。

(2) 標準的な量子計算モデルの可能性と限界の研究

対数領域限定の量子計算モデルについて，ある限定した計算モデルにおいて通常の多項式時間量子計算同様に計算誤りが低減化できることを明らかにした。これにより，マッチゲート計算の計算誤り低減化や対数領域限定の QMA(量子版 NP)の通常の多項式量子計算との等価性を示すことができた。さらに量子対話型証明の QMA システムに事後選択を許したモデルの計算能力が PSPACE と一致することを明らかにした。対話型証明において，一般の量子回路では BQP 完全であるような量子回路の識別問題が，第 2 フーリエ階層という量子回路のクラスに限ると，古典計算機で効率的に検証できることを示した。

(3) 量子分散アルゴリズムの研究

通信計算量理論および分散計算の枠組みにおいて，データベース理論における二つのデータベースの結合を計算する問題などに対して古典プロトコルより効率的な量子プロトコルを構築した。分散計算の枠組みの CONGEST モデルに着目し，行列式など様々な代数的問題を従来のプロトコルより低いラウンド数で解けるプロトコルを構築した。この代数的なアプローチにより，最短経路問題など重要な問題に対するプロトコル計算量も改良した。量子プロトコル理論を深めるために，2 者間通信及び分散計算の枠組みで，計算機科学の中核的な問題である三角形発見問題に対してプロトコルの構築と解析を行なった。2 者間通信では疎グラフ上の三角形発見問題に着目し従来のプロトコルより効率的な量子プロトコルを構築した。分散計算では一般のグラフまで対象を広げて従来のプロトコルの大幅な改良した。量子分散計算の優位性を示すべく，標準的モデルの CONGEST モデルにおいて，古典分散プロトコルよりも高速にネットワーク直径を求める量子分散プロトコルを構築した。もう一つの重要なモデルの LOCAL モデルにおいても，量子論の非局所性に基づく高速な量子プロトコルを開発した。分散計算の中核的な問題である「全対最短経路問題」に対して，最良の古典分散プロトコルより高速な量子分散プロトコルの開発に成功した。帯域幅の限られているモデルにおいて，三角形発見問題を高速に解く量子分散プロトコルを構築できた。クリークを数え上げる問題・複製データの検証問題，グラフの内周やサイクルに関する問題などの効率的な手法を開発することに成功した。量子分散アルゴリズムの研究分野に関しては，世界的に牽引する役割を担っていると考えている。低深度量子回路の量子性を検査する問題や対数領域しか用いない量子アルゴリズムの性質など量子計

算量理論的な性質の究明も行なった。加えて，量子アルゴリズムを考慮する際に生じたアイデアを用いて，各種古典アルゴリズムの開発を行うことができた。

(4) ユニタリ演算識別問題の研究
ユニタリ演算は量子計算における基本演算であり，そのユニタリ演算識別問題は二つのユニタリ演算の候補のうちのいずれかが未知のユニタリ演算として与えられたときにその未知のユニタリ演算が候補のうちのどちらであるかを当てる問題である。この問題に対して，量子質問アルゴリズムの視点から研究を行い，二つのユニタリ演算を識別するのに必要十分な未知のユニタリ演算の数の緊密な上下界を得ることができ，詳細な解析により，二つの量子回路素子の識別の困難さを特徴付けることができる量子回路素子の特徴量を同定することで，任意の二つの量子素子を識別するための必要十分な質問計算量を示した。精緻化した解析によりユニタリ識別問題に対する質問計算量を改善した。

(5) 耐量子暗号の研究
古典決定性鍵暗号化方式において，量子状態平文に対する暗号文を入手可能な攻撃者を考えた場合，攻撃者が暗号化後に平文レジスタにアクセスできれば，任意の方式を攻撃可能であることを示した。量子コンピュータが登場した後の世界においても安全性が担保される暗号系が重要であり，符号ベース暗号でスタンダードモデルにおいて IK-CCA2 を達成する最初の方式を提案した。また，量子コンピュータに対しても困難と予想される RLWE 問題に基づく準同型暗号を用いて応用諸領域に対して高速な秘匿計算方法を構築した。
　また，米国標準技術研究所(NIST)の「量子計算機の攻撃に耐えうる暗号プロトコルの標準化プロジェクト」の有力候補 HQC 公開鍵暗号に基づいた線形関数および大小比較に対する効率的な秘匿計算プロトコルを構成しその安全性を証明した。

(6) 新しい計算モデルにおけるプロトコルの研究
新しい枠組みからプロトコルを開発することを目指して，非許可型コンセンサスプロトコルの不可能性回避方法について，敵対的計算能力に対する耐性限界が信頼できる構成要素を活用することで改善できる可能性を明らかにした。ゲーム理論の観点によりリスク回避型攻撃者に対するプロトコルの安全性を導入し紛失通信等に対して安全性概念間の関係を明らかにした。
　秘匿メッセージ伝達プロトコルにおいて，敵対者の合理性を利用することで，n 本の通信路のうち n-1 本まで敵対者に支配されたとしても(既存設定では不可能であった)完全秘匿性を達成するプロトコルを構成した。マルチパーティ計算の和集合計算に対し，信頼できる第三者を仮定しないで，各参加者の得る利益に関して公平性を実現するプロトコルを提案した。

(7) 量子暗号プロトコルの研究
　秘匿代理量子計算において，クライアントが古典の場合，完全秘匿性を達成不可能であることを証明し，クライアントが量子的であることが本質的であることを示した。またクライアントがサーバに計算の内容を秘匿して量子計算をさせるブラインド量子計算の基本的な設定での不可能性を示し，さらに弱い量子計算モデルによるサンプリングの不可能性も示した。
　量子プロトコルに関しての基礎的研究として，量子計算機を持つと主張するサーバに対する量子計算機を持つかのクライアントによる古典的検証可能性に，報酬の概念を導入するモデルを提案し，ゲーム理論的な形での同課題の解決という新しい方向性を見出した。
　非対話形式の多者間秘匿計算の一つである秘匿同報通信の共有量子絡れ状態を持つ量子版プロトコルが共有乱数を持つ古典版プロコトルに対して通信複雑度の点での優位性を示した。

(8) 古典暗号プロトコルの研究
量子プロトコル理論へ基礎を与えるための古典暗号プロトコル研究でも貢献した。セキュアメッセージ伝達プロトコルについて，複数の独立した敵対者が存在するモデルでは，すべての通信路が支配されたとしてもゲーム理論的な安全性を達成できることを示した。これは，敵対者がすべての資源を支配した場合に自明に安全性が成り立たない古典的な安全性では実現できない結果である。
　また，暗号プロトコルの性質解析で通常利用される全変動距離(Total Variation Distance)に対して，Hellinger 距離という概念を導入する新規解析手法を開発することに成功し，よりタイトな性質評価が行えるようになった。

５．主な発表論文等

〔雑誌論文〕　計83件（うち査読付論文　82件／うち国際共著　15件／うちオープンアクセス　13件）

１．著者名 Go Sato, Takeshi Koshiba, Tomoyuki Morimae	４．巻 18
２．論文標題 Arbitrable blind quantum computation	５．発行年 2019年
３．雑誌名 Quantum Information Processing	６．最初と最後の頁 Article 370
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11128-019-2482-4	査読の有無 有
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 Tushar Kanti Saha, Mayank Rathee, Takeshi Koshiba	４．巻 49
２．論文標題 Efficient private database queries using ring-LWE somewhat homomorphic encryption	５．発行年 2019年
３．雑誌名 Journal of Information Security and Applications	６．最初と最後の頁 Article 102406
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2019.102406	査読の有無 有
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 該当する

１．著者名 Kenji Yasunaga, Takeshi Koshiba	４．巻 11836
２．論文標題 Perfectly secure message transmission against independent rational adversaries	５．発行年 2019年
３．雑誌名 Lecture Notes in Computer Science (GameSec 2019)	６．最初と最後の頁 563-582
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-32430-8_33	査読の有無 有
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 Vikrant Singh, Behrouz Zolfaghari, Chunduri Venkata Dheeraj Kumar, Brijesh Kumar Rai, Khodakhast Bibak, Gautam Srivastava, Swapnoneel Roy, Takeshi Koshiba	４．巻 24
２．論文標題 Generalized M(m,r)-network: A case for fixed message dimensions	５．発行年 2020年
３．雑誌名 IEEE Communications Letters	６．最初と最後の頁 38-42
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LCOMM.2019.2950193	査読の有無 有
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 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 & 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） なし	査読の有無 有
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 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 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 & 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） なし	査読の有無 有
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 Taisuke Izumi, Francois Le Gall, Frederic Magniez	4．巻 154
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 Leibniz International Proceedings in Informatics (STACS 2020)	6．最初と最後の頁 Article 23
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 137
2．論文標題 Average-case quantum advantage with shallow circuits	5．発行年 2019年
3．雑誌名 Leibniz International Proceedings in Informatics (CCC 2020)	6．最初と最後の頁 Article 21
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 Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka	4．巻 795
2．論文標題 Simulation-based receiver selective opening CCA secure PKE from standard computational assumptions	5．発行年 2019年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 570-597
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2019.08.016	査読の有無 有
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 Fuyuki Kitagawa, Takahiro Matsuda, Keisuke Tanaka	4．巻 11923
2．論文標題 Simple and efficient KDM-CCA secure public key encryption	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (ASIACRYPT 2019)	6．最初と最後の頁 97-127
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34618-8_4	査読の有無 有
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 Yusuke Yoshida, Fuyuki Kitagawa, Keisuke Tanaka	4．巻 11923
2．論文標題 Non-committing encryption with quasi-optimal ciphertext-rate based on the DDH problem	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (ASIACRYPT 2019)	6．最初と最後の頁 128-158
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34618-8_5	査読の有無 有
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 Shohei Egashira, Yuyu Wang, Keisuke Tanaka	4．巻 11923
2．論文標題 Fine-grained cryptography revisited	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (ASIACRYPT 2019)	6．最初と最後の頁 637-666
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34618-8_22	査読の有無 有
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 Fuyuki Kitagawa, Takahiro Matsuda, Keisuke Tanaka	4．巻 11694
2．論文標題 CCA security and trapdoor functions via key-dependent-message security	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (CRYPTO 2019)	6．最初と最後の頁 33-64
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26954-8_2	査読の有無 有
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 Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka, Takashi Yamakawa	4．巻 11694
2．論文標題 Adaptively secure and succinct functional encryption: Improving security and efficiency, simultaneously	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (CRYPTO 2019)	6．最初と最後の頁 521-551
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26954-8_17	査読の有無 有
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 Masayuki Tezuka, Xiangyu Su, Keisuke Tanaka	4．巻 11829
2．論文標題 A t-out-of-n redactable signature scheme	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (CANS 2019)	6．最初と最後の頁 470-489
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-31578-8_26	査読の有無 有
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 Tomoyuki Morimae, Takeshi Koshiba	4．巻 19
2．論文標題 Impossibility of perfectly-secure one-round delegated quantum computing for classical client	5．発行年 2019年
3．雑誌名 Quantum Information & Computation	6．最初と最後の頁 214-221
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 有
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 Ei Mon Cho, Lwin San, Takeshi Koshiba	4．巻 8
2．論文標題 Non-transferable proxy re-encryption for multiple groups	5．発行年 2018年
3．雑誌名 International Journal of Space-Based and Situated Computing	6．最初と最後の頁 20-29
掲載論文のDOI（デジタルオブジェクト識別子） 10.1504/IJSSC.2018.091192	査読の有無 有
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 Tushar Kanti Saha, Takeshi Koshiba	4．巻 43
2．論文標題 Outsourcing private equality tests to the cloud	5．発行年 2018年
3．雑誌名 Journal of Information Security and Applications	6．最初と最後の頁 83-98
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2018.09.002	査読の有無 有
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 該当する

1．著者名 Maharage Nisansala Sevwandi Perera, Takeshi Koshiba	4．巻 8
2．論文標題 Achieving Strong Security and Member Registration for Lattice-based Group Signature Scheme with Verifier-local Revocation	5．発行年 2018年
3．雑誌名 Journal of Internet Services and Information Security	6．最初と最後の頁 1-15
掲載論文のDOI（デジタルオブジェクト識別子） 10.22667/JISIS.2018.11.30.001	査読の有無 有
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 Maiki Fujita, Kenji Yasunaga, Takeshi Koshiba	4．巻 11199
2．論文標題 Perfectly Secure Message Transmission Against Rational Timid Adversaries	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (GameSec 2018)	6．最初と最後の頁 127-144
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-01554-1_8	査読の有無 有
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 Maharage Nisansala Sevwandi Perera, Takeshi Koshiba	4．巻 11149
2．論文標題 Achieving Full Security for Lattice-Based Group Signatures with Verifier-Local Revocation	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (ICICS 2018)	6．最初と最後の頁 287-302
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-01950-1_17	査読の有無 有
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 Takeshi Koshiba, Katsuyuki Takashima	4．巻 11396
2．論文標題 New Assumptions on Isogenous Pairing Groups with Applications to Attribute-Based Encryption	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (ICISC 2018)	6．最初と最後の頁 3-19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-12146-4_1	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 Maharage Nisansala Sevwandi Perera, Takeshi Koshiba	4．巻 11226
2．論文標題 Almost-Fully Secured Fully Dynamic Group Signatures with Efficient Verifier-Local Revocation and Time-Bound Keys	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (IDCS 2018)	6．最初と最後の頁 134-147
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-02738-4_12	査読の有無 有
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 Maharage Nisansala Sevwandi Perera, Takeshi Koshiba	4．巻 11125
2．論文標題 Achieving Almost-Full Security for Lattice-Based Fully Dynamic Group Signatures with Verifier-Local Revocation	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (ISPEC 2018)	6．最初と最後の頁 229-247
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-99807-7_14	査読の有無 有
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 Maharage Nisansala Sevwandi Perera, Takeshi Koshiba	4．巻 22
2．論文標題 Zero-Knowledge Proof for Lattice-Based Group Signature Schemes with Verifier-Local Revocation	5．発行年 2019年
3．雑誌名 Lecture Notes on Data Engineering and Communications Technologies (NBiS 2018)	6．最初と最後の頁 772-782
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-98530-5_68	査読の有無 有
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 Maharage Nisansala Sevwandi Perera, Takeshi Koshiba	4．巻 11091
2．論文標題 Achieving Strong Security and Verifier-Local Revocation for Dynamic Group Signatures from Lattice Assumptions	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (STM 2018)	6．最初と最後の頁 3-19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-01141-3_1	査読の有無 有
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 Tomoyuki Morimae, Yuki Takeuchi, Harumichi Nishimura	4．巻 2
2．論文標題 Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy	5．発行年 2018年
3．雑誌名 Quantum	6．最初と最後の頁 106-1-106-30
掲載論文のDOI（デジタルオブジェクト識別子） 10.22331/q-2018-11-15-106	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 Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, Seiichiro Tani	4．巻 120
2．論文標題 Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error	5．発行年 2018年
3．雑誌名 Physical Review Letters	6．最初と最後の頁 200502-1-6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevLett.120.200502	査読の有無 有
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 Akinori Kawachi, Kenichi Kawano, Francois Le Gall, Suguru Tamaki	4．巻 102-D
2．論文標題 Quantum Query Complexity of Unitary Operator Discrimination	5．発行年 2019年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 483-491
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018FCP0012	査読の有無 有
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 Francois Le Gall, Harumichi Nishimura, Ansis Rosmanis	4．巻 126
2．論文標題 Quantum Advantage for the LOCAL Model in Distributed Computing	5．発行年 2019年
3．雑誌名 Leibniz International Proceedings in Informatics (STACS 2019)	6．最初と最後の頁 49:1-49:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.STACS.2019.49	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, Tomoyuki Morimae, Harumichi Nishimura, Yuki Takeuchi	4．巻 117
2．論文標題 Interactive Proofs with Polynomial-Time Quantum Prover for Computing the Order of Solvable Groups	5．発行年 2018年
3．雑誌名 Leibniz International Proceedings in Informatics (MFCS 2018)	6．最初と最後の頁 26:1-26:13
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.MFCS.2018.26	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 Akinori Kawachi, Mitsunori Ogihara, Kei Uchizawa	4．巻 762
2．論文標題 Generalized predecessor existence problems for Boolean finite dynamical systems on directed graphs	5．発行年 2019年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 25-40
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2018.08.026	査読の有無 有
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 該当する

1．著者名 Akinori Kawachi	4．巻 733
2．論文標題 Circuit lower bounds from learning-theoretic approaches	5．発行年 2018年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 83-98
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2018.04.038	査読の有無 有
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 Kenji Yasunaga, Kosuke Yuzawa	4．巻 101-A
2．論文標題 Repeated Games for Generating Randomness in Encryption	5．発行年 2018年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 697-703
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.697	査読の有無 有
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 Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka	4．巻 101-A
2．論文標題 Generic Constructions for Fully Secure Revocable Attribute-Based Encryption	5．発行年 2018年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1456-1472
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.1456	査読の有無 有
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 Fuyuki Kitagawa, Keisuke Tanaka	4．巻 11273
2．論文標題 A Framework for Achieving KDM-CCA Secure Public-Key Encryption	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (ASIACRYPT 2018)	6．最初と最後の頁 127-157
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-03329-3_5	査読の有無 有
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 Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka	4．巻 10820
2．論文標題 Memory Lower Bounds of Reductions Revisited	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (EUROCRYPT 2018)	6．最初と最後の頁 61-90
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-78381-9_3	査読の有無 有
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 Fuyuki Kitagawa, Ryo Nishimaki, Keisuke Tanaka	4．巻 10821
2．論文標題 Obfustopia Built on Secret-Key Functional Encryption	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (EUROCRYPT 2018)	6．最初と最後の頁 603-648
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-78375-8_20	査読の有無 有
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 Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka	4．巻 11035
2．論文標題 Fully Anonymous Group Signature with Verifier-Local Revocation	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (SCN 2018)	6．最初と最後の頁 23-42
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-98113-0_2	査読の有無 有
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 Masayuki Tezuka, Yusuke Yoshida, Keisuke Tanaka	4．巻 11359
2．論文標題 Weakened Random Oracle Models with Target Prefix	5．発行年 2019年
3．雑誌名 Lecture Notes in Computer Science (SecITC 2018)	6．最初と最後の頁 344-357
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-12942-2_26	査読の有無 有
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 T. K. Saha, T. Koshiba	4．巻 10239
2．論文標題 Private conjunctive query over encrypted data	5．発行年 2017年
3．雑誌名 Lecture Notes in Computer Science (AFRICACRYPT 2017)	6．最初と最後の頁 149-164
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-57339-7_9	査読の有無 有
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 T. K. Saha, Mayank, T. Koshiba	4．巻 10359
2．論文標題 Efficient protocols for private database queries	5．発行年 2017年
3．雑誌名 Lecture Notes in Computer Science (DBSec 2017)	6．最初と最後の頁 337-348
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-61176-1_19	査読の有無 有
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 該当する

1．著者名 T. K. Saha, T. Koshiba	4．巻 7
2．論文標題 An efficient privacy-preserving comparison protocol	5．発行年 2018年
3．雑誌名 Lecture Notes on Data Engineering and Communications Technologies (NBiS 2017)	6．最初と最後の頁 553-565
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-65521-5_48	査読の有無 有
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 E. M. Cho, L. San, T. Koshiba	4．巻 7
2．論文標題 Secure non-transferable proxy re-encryption for group membership and non-membership	5．発行年 2018年
3．雑誌名 Lecture Notes on Data Engineering and Communications Technologies (TwCSec 2017)	6．最初と最後の頁 876-887
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-65521-5_79	査読の有無 有
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 T. Ohsawa, N. Kurokawa, T. Koshiba	4．巻 7
2．論文標題 Function secret sharing using Fourier basis	5．発行年 2018年
3．雑誌名 Lecture Notes on Data Engineering and Communications Technologies (TwCSec 2017)	6．最初と最後の頁 865-875
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-65521-5_78	査読の有無 有
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 T. Ito, H. Koizumi, N. Suzuki, I. Kakesu, K. Iwakawa, A. Uchida, T. Koshiba, J. Muramatsu, K. Yoshimura, M. Inubushi, P. Davis	4．巻 7
2．論文標題 Physical implementation of oblivious transfer using optical correlated randomness	5．発行年 2017年
3．雑誌名 Scientific Reports	6．最初と最後の頁 8444-1-8444-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41598-017-08229-x	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 T. K. Saha, T. Koshiba	4．巻 10723
2．論文標題 Privacy-preserving equality test towards big data	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (FPS 2017)	6．最初と最後の頁 95-110
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-75650-9_7	査読の有無 有
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 K. Inasawa, K. Yasunaga	4．巻 100A
2．論文標題 Rational proofs against rational verifiers	5．発行年 2017年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 711-728
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.2392	査読の有無 有
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 A. Kawachi, K. Kawano, F. Le Gall, S. Tamaki	4．巻 10392
2．論文標題 Quantum query complexity of unitary operator discrimination	5．発行年 2017年
3．雑誌名 Lecture Notes in Computer Science (COCOON 2017)	6．最初と最後の頁 309-320
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-62389-4	査読の有無 有
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 A. Kawachi, M. Ogihara, K. Uchizawa	4．巻 83
2．論文標題 Generalized predecessor existence problems for boolean finite dynamical systems	5．発行年 2017年
3．雑誌名 Leibniz International Proceedings in Informatics (MFCS 2017)	6．最初と最後の頁 8:1-8:13
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.MFCS.2017.8	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 D. Doron, F. Le Gall, A. Ta-Shma	4．巻 81
2．論文標題 Probabilistic logarithmic-space algorithms for Laplacian solvers	5．発行年 2017年
3．雑誌名 Leibniz International Proceedings in Informatics (RANDOM 2017)	6．最初と最後の頁 41:1-41:20
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.APPROX-RANDOM.2017.41	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 F. Le Gall, S. Nakajima	4．巻 73
2．論文標題 Multiparty Quantum Communication Complexity of Triangle Finding	5．発行年 2018年
3．雑誌名 Leibniz International Proceedings in Informatics (TQC 2017)	6．最初と最後の頁 6:1-6:11
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.TQC.2017.6	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 F. Le Gall, S. Nakajima	4．巻 79
2．論文標題 Quantum algorithm for triangle finding in sparse graphs	5．発行年 2017年
3．雑誌名 Algorithmica	6．最初と最後の頁 941-959
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00453-016-0267-z	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 T. Morimae, K. Fujii, H. Nishimura	4．巻 95
2．論文標題 Power of one nonclean qubit	5．発行年 2017年
3．雑誌名 Physical Review A	6．最初と最後の頁 042336:1-6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.95.042336	査読の有無 有
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 F. Le Gall, H. Nishimura	4．巻 2017
2．論文標題 Quantum algorithms for matrix products over semirings	5．発行年 2017年
3．雑誌名 Chicago Journal of Theoretical Computer Science	6．最初と最後の頁 1:1-1:25
掲載論文のDOI（デジタルオブジェクト識別子） 10.4086/cjtcs.2017.001	査読の有無 有
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 T. Morimae, H. Nishimura	4．巻 17
2．論文標題 Merlinization of complexity classes above BQP	5．発行年 2017年
3．雑誌名 Quantum Information and Computation	6．最初と最後の頁 959-972
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 有
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 T. M. Thanh, K. Tanaka	4．巻 76
2．論文標題 An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information	5．発行年 2017年
3．雑誌名 Multimedia Tools and Applications	6．最初と最後の頁 13455-13471
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-016-3750-2	査読の有無 有
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 該当する

1．著者名 Y. Wang, K. Tanaka	4．巻 100A
2．論文標題 Generic transformation for signatures in the continual leakage model	5．発行年 2017年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1857-1869
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.1857	査読の有無 有
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 A. Ishida, K. Emura, G. Hanaoka, Y. Sakai, K. Tanaka	4．巻 100A
2．論文標題 Group signature with deniability: How to disavow a signature	5．発行年 2017年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1825-1837
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.1825	査読の有無 有
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 T. M. Thanh, K. Tanaka, L. H. Dung, N. T. Tai, H. N. Nam	4．巻 77
2．論文標題 Performance analysis of robust watermarking using linear and nonlinear feature matching	5．発行年 2018年
3．雑誌名 Multimedia Tools and Applications	6．最初と最後の頁 2901-2920
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-017-4435-1	査読の有無 有
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 該当する

1．著者名 Y. Yoshida, K. Morozov, K. Tanaka	4．巻 10346
2．論文標題 CCA2 Key-Privacy for Code-Based Encryption in the Standard Model	5．発行年 2017年
3．雑誌名 Lecture Notes in Computer Science (PQCrypto 2017)	6．最初と最後の頁 35-50
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-59879-6_3	査読の有無 有
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 K. Yamada, N. Attrapadung, K. Emura, G. Hanaoka, K. Tanaka	4．巻 10493
2．論文標題 Generic constructions for fully secure revocable attribute-based encryption	5．発行年 2017年
3．雑誌名 Lecture Notes in Computer Science (ESORICS 2017)	6．最初と最後の頁 532-551
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-66399-9_29	査読の有無 有
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 F. Kitagawa, R. Nishimaki, K. Tanaka	4．巻 10770
2．論文標題 Simple and generic constructions of succinct functional encryption	5．発行年 2018年
3．雑誌名 Lecture Notes in Computer Science (PKC 2018)	6．最初と最後の頁 187-217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-76581-5_7	査読の有無 有
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 F. Kitagawa, K. Tanaka	４．巻 10769
２．論文標題 Key dependent message security and receiver selective opening security for identity-based encryption	５．発行年 2018年
３．雑誌名 Lecture Notes in Computer Science (PKC 2018)	６．最初と最後の頁 32-61
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-76578-5_2	査読の有無 有
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 Ta Minh Thanh, Keisuke Tanaka	４．巻 75
２．論文標題 The novel and robust watermarking method based on q-logarithm frequency domain	５．発行年 2016年
３．雑誌名 Multimedia Tools and Applicatoins	６．最初と最後の頁 11097-11125
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-015-2836-6	査読の有無 有
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 該当する

１．著者名 Yuyu Wang, Keisuke Tanaka	４．巻 9
２．論文標題 Generic transformations for existentially unforgeable signature schemes in the bounded leakage model	５．発行年 2016年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 1829-1842
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/sec.1436	査読の有無 有
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 Yuyu Wang, Zongyang Zhang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka	４．巻 10032
２．論文標題 How to Obtain Fully Structure-Preserving (Automorphic) Signatures from Structure-Preserving Ones	５．発行年 2016年
３．雑誌名 Lecture Notes in Computer Science (ASIACRYPT 2016)	６．最初と最後の頁 465-495
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-662-53890-6_16	査読の有無 有
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 Ai Ishida, Keita Emura, Goichiro Hanaoka, Yusuke Sakai, Keisuke Tanaka	4．巻 10052
2．論文標題 Group Signature with Deniability: How to Disavow a Signature	5．発行年 2016年
3．雑誌名 Lecture Notes in Computer Science (CANS 2016)	6．最初と最後の頁 228-244
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-48965-0_14	査読の有無 有
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 Akinori Kawachi, Hirotoshi Takebe, Keisuke Tanaka	4．巻 9836
2．論文標題 Lower Bounds for Key Length of k-wise Almost Independent Permutations and Certain Symmetric-Key Encryption Schemes	5．発行年 2016年
3．雑誌名 Lecture Notes in Computer Science (IWSEC 2016)	6．最初と最後の頁 195-211
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-44524-3_12	査読の有無 有
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 Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, Keisuke Tanaka	4．巻 9841
2．論文標題 Signatures Resilient to Uninvertible Leakage	5．発行年 2016年
3．雑誌名 Lecture Notes in Computer Science (SCN 2016)	6．最初と最後の頁 372-390
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-44618-9_20	査読の有無 有
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 Kenji Yasunaga	4．巻 10015
2．論文標題 Error-Correcting Codes Against Chosen-Codeword Attacks	5．発行年 2016年
3．雑誌名 Lecture Notes in Computer Science (ICITS 2016)	6．最初と最後の頁 177-189
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-49175-2_9	査読の有無 有
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 Andris Ambainis, Kazuo Iwama, Masaki Nakanishi, Harumichi Nishimura, Rudy Raymond, Seiichiro Tani, Shigeru Yamashita	4．巻 25
2．論文標題 Quantum Query Complexity of Almost All Functions with Fixed On-set Size	5．発行年 2016年
3．雑誌名 Computational Complexity	6．最初と最後の頁 723-735
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00037-016-0139-6	査読の有無 有
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 該当する

1．著者名 Tomoyuki Morimae, Harumichi Nishimura	4．巻 16
2．論文標題 Quantum interpretations of AWPP and APP	5．発行年 2016年
3．雑誌名 Quantum Information & Computation	6．最初と最後の頁 498-514
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 有
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 Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, Seiichiro Tani	4．巻 55
2．論文標題 Power of Quantum Computation with Few Clean Qubits	5．発行年 2016年
3．雑誌名 Leibniz International Proceedings in Informatics (ICALP 2016)	6．最初と最後の頁 13:1-13:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ICALP.2016.13	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 Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, Harumichi Nishimura	4．巻 55
2．論文標題 Space-Efficient Error Reduction for Unitary Quantum Computations	5．発行年 2016年
3．雑誌名 Leibniz International Proceedings in Informatics (ICALP 2016)	6．最初と最後の頁 14:1-14:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ICALP.2016.14	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 Stacey Jeffery, Robin Kothari, Francois Le Gall, Frederic Magniez	4．巻 76
2．論文標題 Improving Quantum Query Complexity of Boolean Matrix Multiplication Using Graph Collision	5．発行年 2016年
3．雑誌名 Algorithmica	6．最初と最後の頁 1-16
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00453-015-9985-x	査読の有無 有
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 該当する

1．著者名 Stacey Jeffery, Francois Le Gall	4．巻 58
2．論文標題 Quantum Communication Complexity of Distributed Set Joins	5．発行年 2016年
3．雑誌名 Leibniz International Proceedings in Informatics (MFCS 2016)	6．最初と最後の頁 54:1-54:13
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.MFCS.2016.54	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 9888
2．論文標題 Further Algebraic Algorithms in the Congested Clique Model and Applications to Graph-Theoretic Problems	5．発行年 2016年
3．雑誌名 Lecture Notes in Computer Science (DISC 2016)	6．最初と最後の頁 57-70
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-662-53426-7_5	査読の有無 有
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 Tushar Kanti Saha, Takeshi Koshiba	4．巻 10128
2．論文標題 An Enhancement of Privacy-Preserving Wildcards Pattern Matching	5．発行年 2017年
3．雑誌名 Lecture Notes in Computer Science (FPS 2016)	6．最初と最後の頁 145-160
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-51966-1_10	査読の有無 有
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 Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, Takeshi Koshiba	4．巻 11
2．論文標題 Analysis of decreasing squared-sum of Gram-Schmidt lengths for short lattice vectors	5．発行年 2017年
3．雑誌名 Journal of Mathematical Cryptology	6．最初と最後の頁 1-24
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/jmc-2016-0008	査読の有無 有
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 Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, Kenji Yasunaga	4．巻 印刷中
2．論文標題 General constructions of rational secret sharing with expected constant-round reconstruction	5．発行年 2017年
3．雑誌名 The Computer Journal	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1093/comjnl/bxw094	査読の有無 有
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 Tomoyuki Morimae, Harumichi Nishimura, Francois Le Gall	4．巻 17
2．論文標題 Modified Group Non-Membership is in Promise-AWPP relative to group oracles	5．発行年 2017年
3．雑誌名 Quantum Information & Computation	6．最初と最後の頁 242-250
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 有
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 －

〔学会発表〕　計31件（うち招待講演　14件／うち国際学会　23件）

1．発表者名 Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Keisuke Tanaka
2．発表標題 Proper Usage of the Group Signature Scheme in ISO/IEC 20008-2
3．学会等名 2019 ACM Asia Conference on Computer and Communications Security, AsiaCCS 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
Takeshi Koshiba

２．発表標題
Recent Progress in Quantum Computational Cryptography

３．学会等名
The 6th IEEE Conference on Computer Science and Data Engineering, CSDE 2019（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Takeshi Koshiba

２．発表標題
On Public Verifiability for Secure Delegated Quantum Computation

３．学会等名
研究集会「量子計算，ポスト量子暗号，量子符号の融合と深化」（招待講演）

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
The 1st Workshop on Quantum and Classical Cryogenic Devices, Circuits, and Systems （QCCC2019）（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 Protocols（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
Possibility of 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
Hideaki Miyaji, Akinori Kawachi, Atsuko Miyaji

２．発表標題
String commitment schemes with low output locality

３．学会等名
The 14th Asia Joint Conference on Information Security (AsiaJCIS 2019)（国際学会）

４．発表年
2019年

１．発表者名
河内 亮周

２．発表標題
量子攻撃者に対する安全性概念

３．学会等名
電子情報通信学会総合大会企画セッション「量子計算と暗号の発展」（招待講演）

４．発表年
2020年

１．発表者名
Masahito Hayashi, Takeshi Koshiba

２．発表標題
Universal Construction of Cheater-Identifiable Secret Sharing Against Rushing Cheaters Based on Message Authentication

３．学会等名
2018 IEEE International Symposium on Information Theory, ISIT 2018（国際学会）

４．発表年
2018年

１．発表者名
Tomohiro Hayashi, Kenji Yasunaga

２．発表標題
On the List Decodability of Insertions and Deletions

３．学会等名
2018 IEEE International Symposium on Information Theory, ISIT 2018（国際学会）

４．発表年
2018年

１．発表者名
Francois Le Gall, Frederic Magniez

２．発表標題
Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks

３．学会等名
2018 ACM Symposium on Principles of Distributed Computing, PODC 2018（国際学会）

４．発表年
2018年

１．発表者名
Francois Le Gall, Frederic Magniez

２．発表標題
Sublinear-Time Quantum Computation of the Diameter in CONGEST Networks

３．学会等名
22nd Annual Conference on Quantum Information Processing, QIP 2019（国際学会）

４．発表年
2019年

１．発表者名
Maharage Nisansala Sevwandi Perera, Takeshi Koshiba

２．発表標題
A guests managing system with lattice-based verifier-local revocation group signature scheme with time-bound keys

３．学会等名
5th International Conference on Mathematics & Computing, ICMC 2019（国際学会）

４．発表年
2019年

１．発表者名
小柴健史

２．発表標題
安全な代理量子計算

３．学会等名
情報理論研究会「若手研究者のための講演会」@第41回情報理論とその応用シンポジウム，SITA 2018（招待講演）

４．発表年
2018年

１．発表者名
Takeshi Koshiba

２．発表標題
Homomorphic Encrypion and Its Applications

３．学会等名
2018 International Conference for Top and Emerging Computer Scientists, IC-TECS 2018（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
小柴健史

２．発表標題
観測に基づく量子計算と量子優位性

３．学会等名
CREST暗号数理 平成30年度第2回全体会議 チュートリアルワークショップ（招待講演）

４．発表年
2018年

１．発表者名
西村治道

２．発表標題
量子計算量クラスについて

３．学会等名
ImPACT未来開拓研究会2018（招待講演）

４．発表年
2018年

１．発表者名
Francois Le Gall

２．発表標題
Quantum Distributed Computing

３．学会等名
20th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2018)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
T. Koshiba

２．発表標題
Secure Message Transmission against Rational Adversaries

３．学会等名
Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
小柴健史

２．発表標題
Secure Message Transmission : 可能性と限界

３．学会等名
第６回誤り訂正符号のワークショップ（電子情報通信学会 情報理論とその応用サブソサイエティ）（招待講演）

４．発表年
2017年

１．発表者名
小柴健史

２．発表標題
耐量子時代の擬似乱数生成

３．学会等名
Small-workshop on Communications between Academia and Industry for Security (SCAIS 2018)（招待講演）

４．発表年
2018年

１．発表者名
E. M. Cho, T. Koshiba

２．発表標題
Big data cloud deduplication based on verifiable hash convergent group signcryption

３．学会等名
The 3rd IEEE International Conference on Big Data Computing Service and Applications（国際学会）

４．発表年
2017年

１．発表者名
E. M. Cho, T. Koshiba

２．発表標題
Secure SMS transmission based on verifiable hash convergent group signcryption

３．学会等名
The 18th IEEE International Conference on Mobile Data Management (MDM 2017)（国際学会）

４．発表年
2017年

１．発表者名
T. K. Saha, Mayank, Deevashwer, T. Koshiba

２．発表標題
Private comparison protocol and its application to range queries

３．学会等名
The 10th International Conference on Internet and Distributed Computing Systems (IDCS 2017)（国際学会）

４．発表年
2017年

１．発表者名
M. N. S. Perera, T. Koshiba

２．発表標題
Fully dynamic group signature scheme with member registration and verifier-local revocation

３．学会等名
The 4th International Conference on Mathematics and Computing (ICMC 2018)（国際学会）

４．発表年
2018年

１．発表者名
T. Koshiba

２．発表標題
Fourier-based function secret sharing with general access structure

３．学会等名
The 4th International Conference on Mathematics and Computing (ICMC 2018)（国際学会）

４．発表年
2018年

１．発表者名
安永憲司

２．発表標題
暗号技術に対するゲーム理論的なアプローチ

３．学会等名
第9回暗号及び情報セキュリティと数学の相関ワークショップ（招待講演）

４．発表年
2017年

１．発表者名
T. Izumi, F. Le Gall.

２．発表標題
Triangle finding and listing in CONGEST networks

３．学会等名
The 36th ACM Symposium on Principles of Distributed Computing (PODC 2017)（国際学会）

４．発表年
2017年

１．発表者名
Ei Mon Cho, Takeshi Koshiba

２．発表標題
Secure Deduplication in a Multiple Group Signature Setting

３．学会等名
The 31st IEEE International Conference on Advanced Information Networking and Applications (AINA 2017)（国際学会）

４．発表年
2017年

１．発表者名
Tushar Kanti Saha, Takeshi Koshiba

２．発表標題
Private Equality Test using Ring-LWE Somewhat Homomorphic Encryption

３．学会等名
The 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE 2016)（国際学会）

４．発表年
2016年

〔図書〕　計1件

１．著者名 小柴健史，藤井啓祐，森前智行	４．発行年 2017年
２．出版社 コロナ社	５．総ページ数 196（1-18，132-133，159，185-186）
３．書名 観測に基づく量子計算	

〔産業財産権〕

〔その他〕

Workshop on Quantum Protocols の情報は以下から参照できます。
http://www.f.waseda.jp/tkoshiba/wqp2019/

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	西村　治道 (Nishimura Harumichi) (70433323)	名古屋大学・情報学研究科・教授 (13901)	
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・准教授 (13901)	
研究分担者	田中　圭介 (Tanaka Keisuke) (20334518)	東京工業大学・情報理工学院・教授 (12608)	
研究分担者	河内　亮周 (Kawachi Akinori) (00397035)	三重大学・工学研究科・教授 (14101)	
研究分担者	安永　憲司 (Yasunaga Kenji) (50510004)	大阪大学・情報科学研究科・准教授 (14401)	
研究分担者	松本　啓史 (Matsumoto Keiji) (60272390)	国立情報学研究所・情報学プリンシプル研究系・准教授 (62615)	
研究分担者	堀山　貴史 (Horiyama Takashi) (60314530)	埼玉大学・理工学研究科・准教授 (12401)	
研究分担者	小林　弘忠 (Kobayashi HIrotada) (60413936)	国立情報学研究所・情報学プリンシプル系・特任研究員 (62615)	

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1件

国際研究集会	開催年
Workshop on Quantum Protocols	2019年～2019年

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