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　６ 年　 ６ 月 １８ 日現在

機関番号：１３９０１
研究種目：基盤研究(B)（一般）
研究期間：2020～2023
課題番号：２０Ｈ０４１３９

研究課題名（和文）Quantum Algorithms for Large-Scale Quantum Computers: New Horizons and Applications

研究課題名（英文）Quantum Algorithms for Large-Scale Quantum Computers: New Horizons and Applications

研究代表者
ルガル　フランソワ（Le Gall, Francois）

名古屋大学・多元数理科学研究科・教授

研究者番号：５０５８４２９９

交付決定額（研究期間全体）：（直接経費）　　13,300,000円

研究成果の概要（和文）：大規模量子コンピュータの研究能力と応用に関する多くの成果を得た。特筆すべき成果として、高精度化学計算における量子優位性（すなわち、量子コンピュータがスーパーコンピュータよりも速く問題を解決できること）を厳密に証明することに成功した。また、分散型計算における量子優位性を確立するとともに、様々な高速な量子分散型アルゴリズムを構築した。さらに、浅層量子回路の潜在能力を究明し、古典回路に対する量子優位性も明らかにした。

研究成果の学術的意義や社会的意義
20年～30年後に実現が期待される大規模量子コンピュータの活用方法を発展させた。高精度化学計算において、大規模量子コンピュータが通常のコンピュータよりも指数関数的に速く問題を解決できることを示すことにより、顕著な優位性の理論的根拠を与えた。さらに、量子分散アルゴリズムや量子文字列アルゴリズムなど、様々な高速量子アリゴリズムを開発することにより、大規模量子コンピュータの応用を開拓した。

研究成果の概要（英文）：We investigated the computational power and the applications of large-scale quantum computers. We first rigorously established a quantum advantage (i.e., showed that quantum computers can be faster than supercomputers) for fundamental problems such as high-precision chemistry calculations. We developed several fast quantum distributed algorithms and proved a quantum advantage for distributed computing as well. We also investigated the potential of shallow (i.e., low depth) quantum circuits and demonstrated that they can be significantly more powerful than classical shallow circuits.

研究分野：理論計算機科学

キーワード：量子アルゴリズム　量子分散計算　量子計算量理論

１．研究開始当初の背景

Quantum computing is a computation paradigm based on the principles of quantum mechanics that has first been proposed in the 1980's. Early results showed that quantum computers can handle certain computational problems in a way incomparable to classical (i.e., non-quantum) computers. The most celebrated such result is without doubt Shor's algorithm [Shor, SIAM Journal on Computing 1997], which computes the factorization of an integer exponentially faster than all known classical algorithms. This discovery and its consequences to cryptography attracted much attention to quantum computing and to quantum algorithms. Two decades of efforts lead to a better understanding of the power of quantum computers and to the development of a small number of primitives and techniques for quantum algorithm design such as quantum search, quantum walks or quantum phase estimation.

Significant progress has been made in the past five years towards the actual realization of quantum computers: major IT companies (e.g., IBM or Google) announced the creation of small-scale quantum computers; several companies (e.g., Microsoft) launched their own programming languages and compilers for quantum computers. We are entering an era where computation using small-scale quantum computers is now possible and where the construction of medium-scale, and then ultimately even large-scale, quantum computers may finally become within reach.

In view of the significant recent progress made on the hardware side of quantum computing, the main question is not anymore whether a large-scale quantum computer can be constructed, but rather whether it will be worth building such a device, i.e., whether large-scale quantum computers will be useful enough to justify the huge amount of effort, time and investments needed in the next decades for their development. Two decades of works on quantum algorithms have unfortunately not yet given a satisfying answer to this question: known applications of quantum computers (including integer factoring) can hardly be considered as important enough to justify by themselves such a significant cost. Additionally, most theoretical research on quantum algorithms has focused on showing the superiority of quantum computing for abstract models of computations (e.g., query complexity) that are not directly related to the actual performance of quantum algorithms. The most pressing question at this stage of development of quantum computers is thus to discover new, concrete and important problems for which quantum algorithms perform significantly better than the best known classical algorithms.

２．研究の目的

The purpose of this research proposal was to significantly enlarge the realm of applications of quantum algorithms by developing new quantum algorithms and identifying new fields in theoretical computer science for which quantum computation gives significant advantage over classical computation. The three main directions of this proposal were as follows.

A. *New algorithmic applications of quantum search techniques*
   Quantum search, first introduced by Grover in 1996, is still one of the most generic tools for designing quantum algorithms. Besides the apparent simplicity of this technique, algorithms based on quantum search are delicate to design since significant familiarity in both quantum computing and techniques from classical computation is required. Recent breakthroughs [Boroujeni et al., SODA 2018] [Ambainis et al., SODA 2019] have nevertheless shown that quantum algorithms based on quantum

search can lead to some of the most striking applications of quantum algorithms. The first goal of this research proposal was to develop new applications of quantum search techniques. The plan was to especially focus on applications to computational tasks extremely time-consuming for today's computers.

B. *Investigation of quantum distributed algorithms*
Distributed algorithms is a well-established important area in algorithm design. The second research direction of this proposal was to establish the field of quantum distributed algorithms, i.e., to bridge and combine two areas of research in computer science that have mostly been studied independently so far: research on quantum computing and quantum algorithms on one side, and research on distributed computing on the other side. These investigations were expected to lead to the discovery of several new computational tasks for which quantum computation outperforms classical computation and thus cast light on a whole new area of applications for quantum computers.

C. *Average-case analysis of quantum algorithms*
The most traditional measure of performance of algorithms is the running time on the worst-case input. However, such a worst-case input may not be found efficiently, and may actually never be encountered in practice. The field of average-case complexity aims at analyzing the performance of algorithms with respect to random inputs according to some natural distribution. Most of the prior research on quantum algorithms has been done with respect to worst-case complexity. In contrast, our goal was to develop the theory of average-case quantum complexity, and show quantum advantage in this setting as well.

３．研究の方法

Research was conducted in each of the three directions according to the methodology and schedule described in Figure 1 below.

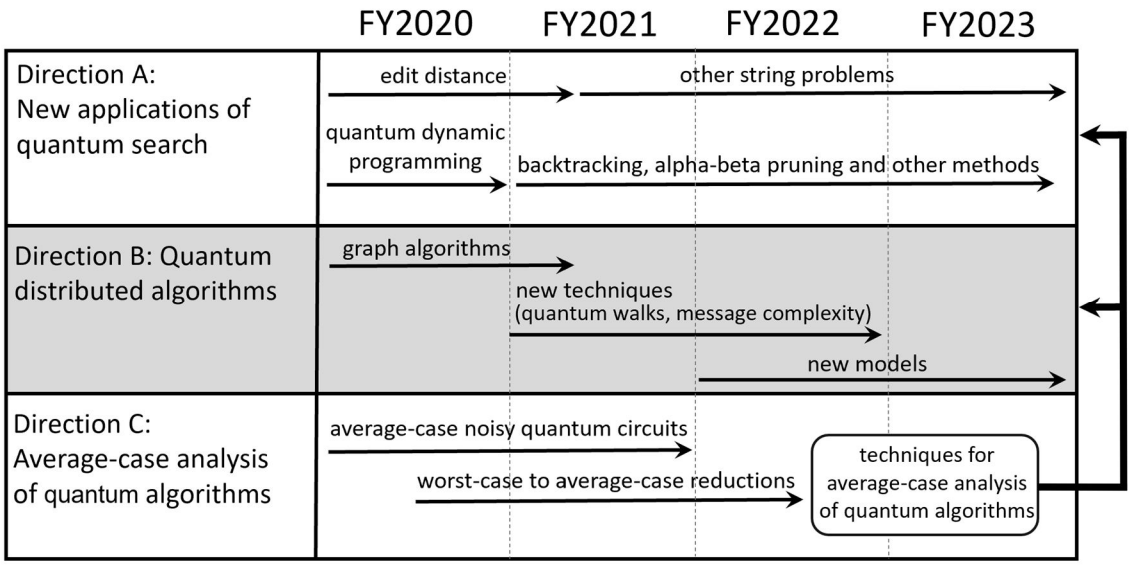

Figure 1: Methodology, Organization and Schedule of our Research Proposal

４．研究成果

We explain below the results obtained during the 4 years of the project. Due to space constraints, we only describe some of the most significant results.

[Quantum string algorithms] We have constructed new quantum algorithms for several important string problems: computing the Longest Common Substring (LCS), computing the Longest Palindrome Substring (LPS) and estimating the Ulam distance. All these fundamental string problems can be classically solved in near linear time. We constructed for the first time sublinear time quantum algorithms, along with quantum lower bounds. Our results shed light on a very surprising fact: Although the classical solutions for LCS and LPS are almost identical, their quantum computational complexities are very different.

[**Dequantization of the Quantum Singular Value Transformation]** The Quantum Singular Value Transformation (QSVT) is a recent technique that gives a unified framework to describe most quantum algorithms discovered so far. We first investigated the hardness of classically simulating the QSVT. A recent result by Chia, Gilyén, Li, Lin, Tang and Wang (STOC 2020) showed that the QSVT can be efficiently "dequantized" for low-rank matrices. We focused on the other main class of matrices considered in applications of the QSVT: sparse matrices. We first showed how to efficiently "dequantize", with arbitrarily small constant precision, the QSVT associated with a low-degree polynomial. We applied this technique to design classical algorithms that estimate, with constant precision, the singular values of a sparse matrix. We also discussed how this dequantization technique may help make progress on the central quantum PCP conjecture.

[**Quantum advantage for quantum chemistry]** We showed that a central computational problem considered by quantum algorithms for quantum chemistry (estimating the ground state energy of a local Hamiltonian when given, as an additional input, a state sufficiently close to the ground state) can be solved efficiently with constant precision on a classical computer. As a complementary result, we proved that with inverse-polynomial precision, the same problem becomes BQP-complete. This gives theoretical evidence for the superiority of quantum algorithms for chemistry, and strongly suggests that said superiority stems from the improved precision achievable in the quantum setting. Then we showed that the BQP-completeness also holds for 2-local physically motivated Hamiltonians on a 2D square lattice or a 2D triangular lattice. Beyond the hardness of estimating the ground state energy, we also showed BQP-hardness persists when considering estimating energies of excited states of these Hamiltonians instead. Those make further steps towards establishing practical quantum advantage in quantum chemistry.

[Quantum distributed algorithms for graph-theoretic problems] The starting point of these investigations was the recent work by Le Gall, Izumi (co-I) and Magniez on quantum distributed computing, which showed that triangle detection by quantum distributed algorithms is easier than triangle listing, while an analogous result is not known in the classical case. We developed a framework for fast quantum distributed clique detection, which improves upon the state-of-the-art for the triangle case, and is also more general, applying to larger clique sizes. Our main technical contribution is a new approach for detecting cliques by encapsulating this as a search task for nodes that can be added to smaller cliques. To extract the best complexities out of our approach, we developed a framework for nested distributed quantum searches, which employs checking procedures that are quantum themselves. Moreover, we showed a circuit-complexity barrier on proving a lower bound of the form $\Omega(n^{3/5})$ for detecting a clique of size p for

any $p \geq 4$, even in the classical (non-quantum) distributed CONGEST setting.

[Lower bounds for quantum distributed algorithms] We investigated quantum multiparty communication complexity in the setting where communication is oblivious. This requirement, which to our knowledge is satisfied by all quantum multiparty protocols in the literature, means that the communication pattern, and in particular the amount of communication exchanged between each pair of players at each round is fixed independently of the input before the execution of the protocol. We showed, for a wide class of functions, how to prove strong lower bounds on their oblivious quantum k-party communication complexity using lower bounds on their two-party communication complexity. We applied this technique to prove tight lower bounds for all symmetric and obtained an optimal lower bound on the oblivious quantum k-party communication complexity of the n-bit Set-Disjointness function. We also showed the tightness of these lower bounds by giving (nearly) matching upper bounds.

[Quantum distributed state synthesis] The generation and verification of quantum states are fundamental tasks for quantum information processing that have recently been investigated by Irani, Natarajan, Nirkhe, Rao and Yuen [CCC 2022], Rosenthal and Yuen [ITCS 2022], Metger and Yuen [FOCS 2023] under the term state synthesis. We have studied this concept from the viewpoint of quantum distributed computing, and especially distributed quantum Merlin-Arthur (dQMA) protocols. We first introduced a novel task, on a line, called state generation with distributed inputs (SGDI). We gave a dQMA protocol for SGDI and utilized this protocol to construct a dQMA protocol for the Set Equality problem studied in prior works. We also showed how to convert any dQMA protocol on an arbitrary network into another dQMA protocol where the verification stage does not require any quantum communication.

[Efficient tests of quantumness] Recently Brakerski, Christiano, Mahadev, Vazirani and Vidick (FOCS 2018) have shown how to construct a test of quantumness based on the learning with errors (LWE) assumption: a test that can be solved efficiently by a quantum computer but cannot be solved by a classical polynomial-time computer under the LWE assumption. This test has led to several cryptographic applications. In particular, it has been applied to producing certifiable randomness from a single untrusted quantum device, self-testing a single quantum device and device-independent quantum key distribution. We have shown that this test of quantumness, and essentially all the above applications, can actually be implemented by a very weak class of quantum circuits: constant-depth quantum circuits combined with logarithmic-depth classical computation. This reveals novel complexity-theoretic properties of this fundamental test of quantumness and gives new concrete evidence of the superiority of small-depth quantum circuits over classical computation.

[Average-case superiority of noisy quantum circuits] We developed methods for analyzing the average-case performance of quantum circuits. While prior works assumed that no noise occurs during the computation, we extended this approach to the much more realistic model of noisy quantum circuits. We showed that even in the presence of noise and even on average inputs, quantum circuits are more powerful than classical circuits, which gives another compelling evidence of the superiority of quantum computing. A key tool to achieve this goal was randomness extraction techniques first developed in [Trevisan, JACM 2001].

５．主な発表論文等

〔雑誌論文〕　計43件（うち査読付論文　43件／うち国際共著　18件／うちオープンアクセス　41件）

１．著者名 Rongcheng Dong, Yuichi Sudo, Taisuke Izumi, Toshimitsu Masuzawa	４．巻 937
２．論文標題 Loosely-stabilizing maximal independent set algorithms with unreliable communications	５．発行年 2022年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 69-84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2022.09.031	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 Naoki Kitamura, Taisuke Izumi	４．巻 105-D(3)
２．論文標題 A Subquadratic-Time Distributed Algorithm for Exact Maximum Matching	５．発行年 2022年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 634-645
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021edp7083	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, Naoki Kitamura, Takamasa Naruse, Gregory Schwartzman	４．巻 -
２．論文標題 Fully Polynomial-Time Distributed Computation in Low-Treewidth Graphs	５．発行年 2022年
３．雑誌名 Proceedings of the 34th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA 2022)	６．最初と最後の頁 11-22
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3490148.3538590	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, Nobutaka Shimizu	４．巻 -
２．論文標題 Hardness Self-Amplification from Feasible Hard-Core Sets	５．発行年 2022年
３．雑誌名 Proceedings of the 63rd Annual Symposium on Foundations of Computer Science (FOCS 2022)	６．最初と最後の頁 543-554
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/FOCS54457.2022.00058	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, Mikito Nanashima	4．巻 -
2．論文標題 Learning Versus Pseudorandom Generators in Constant Parallel Time	5．発行年 2023年
3．雑誌名 Proceedings of the 14th Innovations in Theoretical Computer Science Conference (ITCS 2023)	6．最初と最後の頁 70:1-70:18
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2023.70	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 Eric Allender, Shuichi Hirahara, Harsha Tirumala	4．巻 -
2．論文標題 Kolmogorov Complexity Characterizes Statistical Zero Knowledge	5．発行年 2023年
3．雑誌名 Proceedings of the 14th Innovations in Theoretical Computer Science Conference (ITCS 2023)	6．最初と最後の頁 3:1-3:19
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2023.3	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 該当する

1．著者名 Eric Allender, John Gouwar, Shuichi Hirahara, Caleb Robelle	4．巻 940
2．論文標題 Cryptographic hardness under projections for time-bounded Kolmogorov complexity	5．発行年 2023年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 206-224
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2022.10.040	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 Shuichi Hirahara	4．巻 -
2．論文標題 NP-Hardness of Learning Programs and Partial MCSP	5．発行年 2022年
3．雑誌名 Proceedings of the Symposium on Foundations of Computer Science (FOCS 2022)	6．最初と最後の頁 968-979
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/FOCS54457.2022.00095	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, Mikito Nanashima	4．巻 -
2．論文標題 Finding Errorless Pessiland in Error-Prone Heuristica	5．発行年 2022年
3．雑誌名 Proceedings of the 37th Computational Complexity Conference (CCC 2022)	6．最初と最後の頁 25:1-25:28
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.CCC.2022.25	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	4．巻 -
2．論文標題 Symmetry of Information from Meta-Complexity	5．発行年 2022年
3．雑誌名 Proceedings of the 37th Computational Complexity Conference (CCC 2022)	6．最初と最後の頁 26:1-26:41
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.CCC.2022.26	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 Francois Le Gall, Masayuki Miyamoto and 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 (STACS 2023)	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 －

1．著者名 Atsuya Hasegawa and 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 (ISAAC 2022)	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 and Iu-iong Ng	4．巻 22 (15&16)
2．論文標題 Quantum Approximate Counting for Markov Chains and Application to 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 Francois Le Gall and 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 Latin American Theoretical Informatics Symposium (LATIN 2022)	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 Sevag Gharibian and 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 (STOC 2022)	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 －

1．著者名 Francois Le Gall, Harumichi Nishimura and 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 (TQC 2021)	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 Shuichi Hirahara and 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 (MFCS 2021)	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 Atsuya Hasegawa and Francois Le Gall	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 (ISAAC 2021)	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 Francois Le Gall and Masayuki Miyamoto	4．巻 2021
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 (ISAAC 2021)	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 Aleksandrs Belovs, Arturo Castellanos, Francois Le Gall, Guillaume Malod and Alexander A. Sherstov	4．巻 21(15&16)
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 and 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 (ITCS 2022)	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 Keren Censor-Hillel, Orr Fischer, Francois Le Gall, Dean Leitersdorf and 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 (ITCS 2022	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 Naoki Kitamura, Hirotaka Kitagawa, Yota Otachi, Taisuke Izumi	4．巻 34(5)
2．論文標題 Low-congestion shortcut and graph parameters	5．発行年 2021年
3．雑誌名 Distributed Computing	6．最初と最後の頁 349-365
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00446-021-00401-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 Shuichi Hirahara	4．巻 -
2．論文標題 Average-case hardness of NP from exponential worst-case hardness assumptions	5．発行年 2021年
3．雑誌名 Proceedings of the 53rd ACM SIGACT Symposium on Theory of Computing (STOC)	6．最初と最後の頁 292-302
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3406325.3451065	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, Rahul Ilango, Bruno Loff	4．巻 -
2．論文標題 Hardness of Constant-round Communication Complexity	5．発行年 2021年
3．雑誌名 Proceedings of the 36th Computational Complexity Conference (CCC 2021	6．最初と最後の頁 31:1--31:30
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.CCC.2021.31	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 Eric Allender, John Gouwar, Shuichi Hirahara, Caleb Robelle	4．巻 -
2．論文標題 Cryptographic Hardness Under Projections for Time-Bounded Kolmogorov Complexity	5．発行年 2021年
3．雑誌名 Proceedings of the 32nd International Symposium on Algorithms and Computation (ISAAC 2021)	6．最初と最後の頁 54:1-54:17
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ISAAC.2021.54	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 Mahdi Cheraghchi, Shuichi Hirahara, Dimitrios Myrisiotis, Yuichi Yoshida	4．巻 -
2．論文標題 One-tape Turing machine and branching program lower bounds for MCSP	5．発行年 2021年
3．雑誌名 Proceedings of the 38th International Symposium on Theoretical Aspects of Computer Science	6．最初と最後の頁 23:1-23:19
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.STACS.2021.23	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 Lijie Chen, Shuichi Hirahara, Neekon Vafa	4．巻 -
2．論文標題 Average-Case Hardness of NP and PH from Worst-Case Fine-Grained Assumptions	5．発行年 2022年
3．雑誌名 Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)	6．最初と最後の頁 45:1--45:16
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2022.45	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 Shuichi Hirahara, Rahul Santhanam	4．巻 -
2．論文標題 Excluding PH Pessiland	5．発行年 2022年
3．雑誌名 Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)	6．最初と最後の頁 85:1--85:25
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2022.85	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 Shuichi Hirahara, Rahul Santhanam	4．巻 -
2．論文標題 Errorless Versus Error-Prone Average-Case Complexity	5．発行年 2022年
3．雑誌名 Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)	6．最初と最後の頁 81:1-84:23
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ITCS.2022.84	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 and 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 Computing and Combinatorics Conference (COCOON 2020)	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 Dhawal Jethwani, Francois Le Gall and 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 (MFCS 2020)	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 Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura and Ami Paz	4．巻 -
2．論文標題 Brief Announcement: Distributed Quantum Proofs for Replicated Data	5．発行年 2020年
3．雑誌名 Proceedings of the 34th International Symposium on Distributed Computing (DISC 2020)	6．最初と最後の頁 43:1-43:3
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.DISC.2020.43	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 Keren Censor-Hillel, Orr Fischer, Tzlil Gonen, Francois Le Gall, Dean Leitersdorf and Rotem Oshman	4．巻 -
2．論文標題 Fast Distributed Algorithms for Girth, Cycles and Small Subgraphs	5．発行年 2020年
3．雑誌名 Proceedings of the 34th International Symposium on Distributed Computing (DISC 2020)	6．最初と最後の頁 33:1-33:17
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.DISC.2020.33	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 Keren Censor-Hillel, Francois Le Gall and Dean Leitersdorf	4．巻 -
2．論文標題 On Distributed Listing of Cliques	5．発行年 2020年
3．雑誌名 Proceedings of the 39th ACM Symposium on Principles of Distributed Computing (PODC 2020)	6．最初と最後の頁 474-482
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3382734.3405742	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 Keren Censor-Hillel, Yi-Jun Chang, Francois Le Gall and Dean Leitersdorf	4．巻 -
2．論文標題 Tight Distributed Listing of Cliques	5．発行年 2021年
3．雑誌名 Proceedings of the 32nd ACM-SIAM Symposium on Discrete Algorithms (SODA 2021)	6．最初と最後の頁 2878-2891
掲載論文のDOI（デジタルオブジェクト識別子） 10.1137/1.9781611976465.171	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 Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura and 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 12th Innovations in Theoretical Computer Science Conference (ITCS 2021)	6．最初と最後の頁 8:1-28:20
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 Taisuke Izumi, Yota Otachi	4．巻 -
2．論文標題 Sublinear-Space Lexicographic Depth-First Search for Bounded Treewidth Graphs and Planar Graphs	5．発行年 2020年
3．雑誌名 Proceedings of the 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)	6．最初と最後の頁 67:1-67:17
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.ICALP.2020.67	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, Nobutaka Shimizu	4．巻 -
2．論文標題 Nearly Optimal Average-Case Complexity of Counting Bicliques Under SETH	5．発行年 2021年
3．雑誌名 Proceedings of the 32nd ACM-SIAM Symposium on Discrete Algorithms (SODA 2021)	6．最初と最後の頁 2346-2365
掲載論文のDOI（デジタルオブジェクト識別子） 10.5555/3458064.3458204	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	4．巻 -
2．論文標題 Characterizing Average-Case Complexity of PH by Worst-Case Meta-Complexity	5．発行年 2020年
3．雑誌名 Proceedings of the 61th IEEE Annual Symposium on Foundations of Computer Science (FOCS 2020)	6．最初と最後の頁 50-60
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/FOCS46700.2020.00014	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	4．巻 -
2．論文標題 Non-Disjoint Promise Problems from Meta-Computational View of Pseudorandom Generator Constructions	5．発行年 2020年
3．雑誌名 Proceedings of the 35th Computational Complexity Conference (CCC 2020)	6．最初と最後の頁 20:1-20:47
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.CCC.2020.20	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 Shuichi Hirahara	4．巻 -
2．論文標題 Unexpected hardness results for Kolmogorov complexity under uniform reductions	5．発行年 2020年
3．雑誌名 Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2020)	6．最初と最後の頁 1038-1051
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3357713.3384251	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, Osamu Watanabe	4．巻 -
2．論文標題 On Nonadaptive Security Reductions of Hitting Set Generators	5．発行年 2020年
3．雑誌名 Proceedings of the International Conference on Randomization and Computation (RANDOM 2020)	6．最初と最後の頁 15:1--15:14
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.APPROX/RANDOM.2020.15	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19件（うち招待講演　6件／うち国際学会　7件）

1．発表者名 Sevag Gharibian, Ryu Hayakawa, Francois Le Gall and 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 (QIP 2023)（国際学会）
4．発表年 2023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 (ADGA 2022)（招待講演）（国際学会）

４．発表年
2023年

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

２．発表標題
ガイド付きローカルハミルトニアン問題の計算複雑性の進展

３．学会等名
第47回量子情報技術研究会

４．発表年
2022年

１．発表者名
Francois Le Gall, Masayuki Miyamoto, Harumichi Nishimura

２．発表標題
Distributed Merlin-Arthur Synthesis of Quantum States and Its Applications

３．学会等名
第47回量子情報技術研究会

４．発表年
2022年

１．発表者名
Francois Le Gall, Daiki Suruga

２．発表標題
多人数の量子通信複雑性における新しい手法

３．学会等名
第47回量子情報技術研究会

４．発表年
2022年

１．発表者名
Francois Le Gall

２．発表標題
Theoretical Foundations of Quantum Advantage

３．学会等名
Q2B 2022（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Francois Le Gall, Masayuki Miyamoto, Harumichi Nishimura

２．発表標題
分散量子対話型証明

３．学会等名
第６回量子ソフトウェア研究会

４．発表年
2022年

１．発表者名
Francois Le Gall, Daiki Suruga

２．発表標題
Bounds on oblivious multiparty quantum communication complexity

３．学会等名
第６回量子ソフトウェア研究会

４．発表年
2022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
Rongcheng Dong, Yuichi Sudo, Taisuke Izumi, Toshimitsu Masuzawa

２．発表標題
Loosely-Stabilizing Maximal Independent Set Algorithms with Unreliable Communications

３．学会等名
23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2021)（国際学会）

４．発表年
2021年

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

２．発表標題
Distributed Quantum Proofs for Replicated Data

３．学会等名
第一回量子ソフトウェア研究会

４．発表年
2020年

１．発表者名
宮本昌幸, 岩村 雅一, 黄瀬浩一, Francois Le Gall

２．発表標題
Quantum Speedup for the Minimum Steiner Tree Problem

３．学会等名
第一回量子ソフトウェア研究会

４．発表年
2020年

１．発表者名
Francois Le Gall

２．発表標題
浅層量子回路による平均量子優位性

３．学会等名
第19回情報科学技術フォーラム(FIT2020)（招待講演）

４．発表年
2020年

１．発表者名
Distributed Quantum Proofs for Replicated Data

２．発表標題
Pierre Fraigniaud, Francois Le Gall, Harumichi Nishimura and Ami Paz

３．学会等名
24th Annual Conference on Quantum Information Processing (QIP 2021)（国際学会）

４．発表年
2021年

１．発表者名
Francois Le Gall

２．発表標題
Tight Distributed Listing of Cliques

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（招待講演）

４．発表年
2021年

１．発表者名
Francois Le Gall

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

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

４．発表年
2021年

１．発表者名
Francois Le Gall, 長谷川　敦哉

２．発表標題
ノイズ付き浅層回路による量子計算の優位性

３．学会等名
第2回量子ソフトウェア研究会

４．発表年
2021年

１．発表者名
Shinji Ito, Shuichi Hirahara, Tasuku Soma, Yuichi Yoshida

２．発表標題
Tight First- and Second-Order Regret Bounds for Adversarial Linear Bandits

３．学会等名
Conference on Neural Information Processing Systems (NeurIPS 2020)

４．発表年
2020年

〔図書〕　計0件

〔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	泉　泰介 (Izumi Taisuke) (20432461)	大阪大学・大学院情報科学研究科・准教授 (14401)	
研究分担者	平原　秀一 (Shuichi Hirahara) (80848440)	国立情報学研究所・情報学プリンシプル研究系・准教授 (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			
ドイツ	パーダーボルン大学			
米国	ラトガーズ大学			
イスラエル	イスラエル工科大学	テルアビブ大学		
ラトビア	ラトビア大学			
フランス	パリ大学	CNRS		
英国	オックスフォード大学			