Computer Science Project: Report 2018-2019

I. INTRODUCTION

Our group has witnessed some changes over the last year. Troy Lee has moved to University of Technology Sydney (UTS), Australia. Joe Fitzsimons, who has had close associations with the CS group, has moved to his own startup 'Horizon Quantum Computing'. Anurag Anshu and Priyanka Mukhopadhyay have graduated. Pranab Sen (TIFR, India) and Marco Tomamichel (UTS, Australia) have been added to our long term visiting researchers program. Two new RFs, Maciej Obremski and Patrick Rebentrost (senior RF) have joined our group.

We have started some projects in collaboration with industry and secured a grant with Baidu, a major technology company in China. We have also secured a *VanQuTe* grant, a joint grant between a few Singapore and French institutes.

II. GROUP MEMBERS AND VISITORS

A. Permanent group members

1. **Principal Investigators**:
   Divesh Aggarwal
   Rahul Jain
   Hartmut Klauck
   Miklos Santha.

2. **Research Fellows**:
   Li Jianwei
   Maciej Obremski
   Patrick Rebentrost
   Ansis Rosmanis
   Naqueeb Warsi.

3. **Ph.D students**:
   Naresh B. Goud
   Srijita Kundu
   Upendra Kapshikar
   Debbie Lim
   Maharshi Ray
   Siyi Yang.

B. Visitors

1. **Regular Visiting Researchers**:
   Itai Arad, Technion (2 months)
   Dmitry Gavinsky, Czech Academy of Sciences (4 months)
   Gábor Ivanyos, Hungarian Academy of Sciences (3 months)
   Antoine Joux, Université Pierre et Marie Curie (1 month)
   Iordanis Kerenidis, CNRS, Université Paris Diderot (2 months)
   Troy Lee, University of Technology Sydney (2 months, started in 2019)
   Serge Massar, FNRS, Université Libre de Bruxelles (1 month)
   Pranab Sen, Tata Institute of Fundamental Research (1 month, started in 2019)
   Marco Tomamichel, University of Technology Sydney (1 month, started in 2019)
   Thomas Vidick, Caltech (1 month).

2. **Interns**:
   Alper Cakan, Joao Miguel Lourenco Ribeiro, Lai Wenxing, Kyriakos Katsamaktsis, Kunal Mittal, Zichuan Wei, Jevgenijs Vihrovs, Zuo Huijuan, Rajendra Kumar, Rishabh Batra, Wu Xinyu, Wang Mingyuan, Liu Yupan, Joao Miguel Lourenco Ribeiro.

3. **Temporary visitors**:
   Ronald Cramer, Anupam Prakash, Venkatesh Srinivasan, Priyanka Mukhopadhyay, Anurag Anshu, Yassine Hamoudi, Felix Klingelhoefer, Michel de Rougemont, Elisa Celis, Nisheeth Vishnoi, Jianwei Li, Aarthi Sundaram, Alexander Belov, Tomasz Kazana, Prakash Anupam, Maciej Skorski, Ronald Cramer, Yassine Hamoudi, Luisa Siniscalchi, Stefan Dziembowski, Noah Stephens-Davidowitz, Jean-Claude Bajard, Yassine Hamoudi, Abel Molina, Yanlin Chen, Samuel Bosch, Shen Yixin, Akshayaram Srinivasan, Jon Allcock, Robert Huang, Luisa Siniscalchi.

III. RESEARCH HIGHLIGHTS

A. Algorithms and Complexity

1. In [34] we initiate the study of quantum races, games where two or more quantum computers compete to solve a computational problem. While the problem of dueling algorithms has been studied for classical deterministic algorithms the quantum case presents additional sources of uncertainty for the players. The foremost among these is that players do not know if they have solved the problem until they measure their quantum state. This question of "when to measure?" presents a very interesting strategic problem. We develop a game- theoretic model of a multiplayer quantum race, and find an approximate Nash equilibrium where all players play the same strategy. In the two-party case, we further show that this strategy is nearly optimal in terms of payoff among all symmetric Nash equilibria. A key role in our analysis of quantum races is played by a more tractable version of the game where there is no payout on a tie; for such races we completely characterize the Nash equilibria in the two-party case. One application of our results is to the stability of the Bitcoin protocol when mining is done by quantum computers. Bitcoin mining is a race to solve a computational search problem, with the winner gaining the right to create a new block. Our results inform the strategies that eventual quantum miners should use, and also indicate that the collision probability—the probability that two miners find a new block at the same time—would not be too high in the case of quantum miners. Such collisions are undesirable as they lead to forking of the Bitcoin blockchain.

2. In [30] we extended the results of our earlier conference paper to algorithms over the real and complex numbers, making them applicable not only in multivariate cryptography but also to problems from quantum computing. The computational problems addressed include simultaneous isometry of two tuples of matrices as well as simultaneously symmetrizing and skew-symmetrizing matrices. The methods are based on the theory of the $*$-algebras.

3. Optimization is a cornerstone of machine learning and artificial intelligence. Within a research collaboration with Baidu, a research project on quantum optimization was initiated. In particular, we investigate optimization methods based on multiplicative weight updates with the application to certain kinds of neural networks [38].

4. Near-term quantum computers are characterized by large error rates, the absence of error correction, and relatively few quantum gates. Current research includes algorithms for such near-term quantum computers using the variational-hybrid and QAOA approaches. We investigate performing conjugate gradient descent on small quantum devices and using such devices as a heuristic solver for minimising convex functions with constraints [39].

B. Information Theory, Communication Complexity and Query Complexity

1. The logarithm of the rank of the communication matrix M_F ($M_F(x,y) = F(x,y)$) forms a lower bound on the deterministic communication complexity $D(F)$ of F. The well-known and long standing *Log-Rank Conjecture* posits that $D(F) = \text{polylog}(\text{rank}(M(F))$. A natural randomized analogue is the *Log-Approximate-Rank Conjecture*: $R(F) = \text{polylog}(\text{arank}(M_F))$, where $\text{arank}(M_F)$ is approximate rank of $M(F)$ (with constant ℓ_1 approximation) and $R(F)$ is the randomized communication complexity of F (with constant worst-case error).

   In a recent breakthrough work, Chattopadhyay, Mande and Sherif establish that Log-Approximate-Rank Conjecture is false by exhibiting a function with an exponential separation between the randomized communication complexity (with constant error) and Log-Approximate-Rank. The work by Chattopadhyay, Mande and Sherif asked if their function had implications for the following *Quantum Log-Approximate-Rank Conjecture*: $Q(F) = \text{polylog}(\text{arank}(M_F))$, where $Q(F)$ is the quantum communication complexity of F.

   In [10], we prove that Quantum Log-Approximate-Rank Conjecture is false as well using the same function as used by Chattopadhyay, Mande and Sherif.

2. Characterising unknown quantum states and measurements is a fundamental problem in quantum information processing. In [23], we provide a novel scheme to self-test local quantum systems using non-contextuality inequalities. Our work leverages the graph-theoretic framework for contextuality introduced by Cabello, Severini, and Winter, combined with tools from mathematical optimisation that guarantee the unicity of optimal solutions. As an application, we show that the celebrated Klyachko-Can-Binicioglu-Shumovsky inequality and its generalization to contextuality scenarios with odd n-cycle compatibility relations admit robust self-testing.

3. This work [15] concerns the problem of *quantum measurement compression* with side information in the one-shot setting with shared-randomness. In this problem, Alice shares a pure quantum state with Bob and the reference system. She performs a measurement on her registers and wishes to communicate the outcome to Bob using shared-randomness and classical communication. The outcome that Bob receives must be correctly correlated with the reference system and his own registers. Our goal is to concurrently minimize the classical communication and shared-randomness cost.

   The suggested protocol presented in this work is based on *convex-split* and position-based decoding. The communication is upper bounded in terms of smooth max and hypothesis testing relative entropies.

   A second protocol addresses the task of strong randomness extraction in the presence of quantum side information. The protocol provides an error guarantee in terms of relative entropy (as opposed to trace distance) and extracts close to the optimal number of uniform bits. As an application, we provide a new achievability result for the task of quantum measurement compression without feedback, in which Alice does not need to know the outcome of the measurement. The result achieves the optimal number of bits communicated and the required number of bits of shared-randomness, for the same task in the asymptotic and i.i.d. setting.

4. This work [25] addresses two problems in the context of two-party communication complexity of functions. First, it concludes the line of research, which can be viewed as demonstrating qualitative advantage of quantum communication in the three most common communication 'layouts': two-way interactive communication; one-way communication; simultaneous message passing (SMP). We demonstrate a functional problem, whose communication complexity is $O(\log^2(n))$ in the quantum version of SMP and $\Omega(\sqrt{n})$ in the classical (randomized) version of SMP.

   Second, this work contributes to understanding the power of the weakest commonly studied regime of quantum communication: SMP with quantum messages and without shared randomness (the latter restriction can be viewed as a somewhat artificial way of making the

quantum model 'as weak as possible'). Our function has an efficient solution in this regime as well, which means that even lacking shared randomness, quantum SMP can be exponentially stronger than its classical counterpart with shared randomness.

5. In [26] we show that for any relation $f \subseteq \{0,1\}^n \times S$ and any partial Boolean function $g : \{0,1\}^m \to \{0,1,*\}$, $R_{1/3}(f \circ g^n) \in \Omega(R_{4/9}(f) \cdot \sqrt{R_{1/3}(g)})$. Here $R_\epsilon(\cdot)$ stands for the bounded-error randomized query complexity with error at most ϵ and $f \circ g^n \subseteq \{0,1\}^{mn} \times S$ denotes the composition of f with n instances of g. The new composition theorem is optimal, at least, for the general case of relational problems: A relation f_0 and a partial Boolean function g_0 are constructed, such that $R_{4/9}(f_0) \in \Theta(\sqrt{n})$, $R_{1/3}(g_0) \in \Theta(n)$ and $R_{1/3}(f_0 \circ g_0^n) \in \Theta(n)$. The theorem is proved via introducing a new complexity measure, max-conflict complexity, denoted by $\bar{\chi}(\cdot)$. Its investigation shows that $\bar{\chi}(g) \in \Omega(\sqrt{R_{1/3}(g)})$ for any partial Boolean function g and $R_{1/3}(f \circ g^n) \in \Omega(R_{4/9}(f) \cdot \bar{\chi}(g))$ for any relation f, which readily implies the composition statement. It is further shown that $\bar{\chi}(g)$ is always at least as large as the sabotage complexity of g.

C. Coding Theory and Cryptography

1. In privacy amplification, two mutually trusted parties aim to amplify the secrecy of an initial shared secret X in order to establish a shared private key K by exchanging messages over an insecure communication channel. If the channel is authenticated the task can be solved in a single round of communication using a strong randomness extractor; choosing a quantum-proof extractor allows one to establish security against quantum adversaries. In the case that the channel is not authenticated, Dodis and Wichs (STOC09) showed that the problem can be solved in two rounds of communication using a non-malleable extractor, a stronger pseudo-random construction than a strong extractor.

   In [1], we give the first construction of a non-malleable extractor that is secure against quantum adversaries. The extractor is based on a construction by Li (FOCS12), and is able to extract from source of min-entropy rates larger than 1/2. Combining this construction with a quantum-proof variant of the reduction of Dodis and Wichs, shown by Cohen and Vidick (unpublished), we obtain the first privacy amplification protocol secure against active quantum adversaries.

2. In [5] we obtain the first continuous information-theoretic non-malleable codes in constant split-state model. As a generalization of error-correcting codes, non-malleable codes guarantee that if the adversary modifies the codeword, then it decodes to either the original message or a completely independent output. We further generalize into continuous non-malleable codes where now we allow the adversary to tamper multiple times. It was known to be impossible to construct information-theoretic continuous non-malleable codes when we split the codeword into two separate parts. While there are known constructions of non-malleable codes in the literature, it was previously unknown whether one can construct continuous non-malleable codes that are split into more than two parts. Our construction allows the adversary to tamper continuously with our codes and yet, either she gets detected, receives the original codeword back, or obtains some unrelated codewords, when we split the codes into eight separate parts.

3. A prominent application of quantum cryptography is the distribution of cryptographic keys that are provably secure. Recently, such security proofs were extended by Vazirani and Vidick (Physical Review Letters, 113, 140501, 2014) to the device-independent (DI) scenario, where the users do not need to trust the integrity of the underlying quantum devices. The protocols analyzed by them and by subsequent authors all require a sequential execution of N multiplayer games, where N is the security parameter. In [33], we prove unconditional security of a protocol where all games are executed in parallel. Besides decreasing the number of time-steps necessary for key generation, this result reduces the security requirements for DI-QKD by allowing arbitrary information leakage of each user's inputs within his or her

lab. To the best of our knowledge, this is the first parallel security proof for a fully device-independent QKD protocol. Our protocol tolerates a constant level of device imprecision and achieves a linear key rate.

D. Hamiltonian Complexity

1. In [19] we have shown how a local Hamiltonian can be learned from taking expectation values of local observables in a steady state of the Hamiltonian, or from its long time dynamics. Unlike other competing approaches for learning Hamiltonians, our method is highly scalable as it only requires local measurement of correlations of Pauli matrices, together with a simple classical post-processing. It can also be applied locally to learn the Hamiltonian of a subsystem. Interestingly, as it relies on the non-commutativity of quantum observables, it is purely quantum without a classical counterpart. Moreover, in several cases, it can shown to outperform the equivalent classical algorithms.

   We are currently working to generalize this approach in two directions: Firstly, to open systems, which enables one to learn the underlying Linbladian from its steady state. The other direction aims at learning commuting Hamiltonians, where our technique has to be combined with classical techniques. Both these directions are now at a advanced stage, nearing publication.

2. In [7] we have managed to prove a subvolume law for the ground state of 2D, frustration-free spin systems with a local spectral gap. This is can be seen as breakthrough with respect to the well-known and long-standing conjecture that gapped ground states of local spin systems satisfy an area-law of the entanglement entropy. Our method relies on the AGSP framework, which was used previously to tackle the 1D case.

   Current work underway is to generalize it to frustrated systems, and try to weaken the local gap condition to a global spectral gap.

IV. TEACHING AND OUTREACH

A. Teaching

1. Divesh Aggarwal: *Topics in Computer Science: Pseudorandomness* (CS6285), NUS, Fall, 2018 and *Computational Complexity* (CS5230), NUS, Spring, 2019.

2. Naresh B. Goud: TA for *Quantum Computing* (CS4268), NUS, Spring 2019.

3. Rahul Jain: *Quantum Computing* (CS4268), NUS, Spring 2019 and *Introduction to Information Theory* (CS3236), Spring 2018.

4. Ansis Rosmanis: *Quantum Algorithms* (QT5201Q), NUS, Fall 2018.

B. Outreach

1. Naresh B. Goud: Lecturer and volunteer for the QCamp-2019.

2. Patrick Rebentrost: CQT11 Colloquium presentation (January 2019) and National Supercomputing Center (NSCC) board meeting presentation on quantum computing (April 2019).

V. FINANCE AND EXPENDITURE

Our expenditure last year has been at the usual rate (around 600 K SGD per year) and we have a fund balance of close to 1.5 million SGD to be spent till March 2020. In addition we have a *VanQuTe* grant (amount 144 K, period 2019-2021, refer to section VI B) and a grant from Baidu (amount 180 K SGD, period April 2019 - January 2020, refer to section VI B).

VI. APPENDIX

A. Invited and contributed talks

1. Divesh Aggarwal

   Invited talk in the workshop on *Elliptic curve cryptography* in November 2018 in Osaka, Japan.
   Invited talk in the workshop on *Fine grained approximation algorithms and complexity* in May 2019 in Bertinoro, Italy.

2. Itai Arad

   Invited talk at the *Entanglement, Integrability and Topology in Many-Body Systems* Workshop, CRM, Montreal, Canada, Sep 2018.
   Invited talk at the *Quantum Connections Symposium*, Jerusalem, May, 2019.

3. Rahul Jain

   Invited talk at the *International Conference on Signal Processing and Communications (SPCOM)*, July 2018, Indian Institute of Science (IISC), Bangalore, India.
   Invited talk at the *TCS Research and Innovation Quantum Computing Symposium*, I.I.T Mumbai, India, 2019.

4. Maciej Obremski

   Invited talk at the *Workshop on Modern Trends in Cryptography*, June 13-14, 2019, Nanyang Technological University, Singapore.

5. Maharshi Ray

   Contributed talk at *ITCS2019*, Sand Diego, January 1012 2019.

6. Patrick Rebentrost

   Invited talk at *QML+*, September 2018, Innsbruck, Austria.

7. Miklos Santha

   Invited talk at *7th French - Israeli FILOFOCS workshop*, Paris, France 3-5 October 2017.

   Contributed talk at *1st QuantERA ERA-NET QuantAlgo workshop*, Paris, France, 25-28 September 2018.

B. Grants and Awards

1. Rahul Jain is a co-PI for the *NRF2017-NRF-ANR004 VanQuTe* grant, a joint grant between Singapore and French institutes. Amount 144 K SGD. Period 2019-2021.

2. Miklos Santha is main PI for the Research Collaboration Agreement between Baidu and NUS on *Quantum algorithms for search, optimization and algebraic problems.* Amount 180 K SGD. Period April 2019 - January 2020.

C. Professional activities

1. Divesh Aggarwal served on the PC of NutMIC 2019, INDOCRYPT 2019, EUROCRYPT 2020.

2. Rahul Jain served on the PC of QIP 2018, TQC 2018 and on the editorial board of *Journal of Computer and System Sciences* (JCSS).

3. Iordanis Kerenidis served on the editorial board of *International Journal of Quantum Information* (IJQI).

4. Troy Lee

   (a) Co-Organizer of *Workshop on cryptography in the quantum age* held at the Stellenbosch Institute for Advanced Study.

   (b) Served on the Program Committees of QIP 2019, Conference on Computational Complexity 2019, and AQIS 2019.

5. Miklos Santha

   (a) Member of the steering committee of Fundamentals of Computation Theory.

   (b) Member of the editorial board of International Journal of Quantum Information.

   (c) Member of the PC of Quantum Technology International Conference, Paris, 2018.

D. Miscellaneous

1. Naresh B. Goud visited Institute for quantum computing (IQC), Waterloo as exchange student for 5 months from August 2018- December 2018.

2. Rahul Jain visited Tata Institute of Fundamental Research (TIFR), Mumbai India as *VAJRA* Adjunct Faculty.

VII. PUBLICATIONS AND PREPRINTS

[1] D. Aggarwal, K.-M. Chung, H.-H. Lin, and T. Vidick. A quantum-proof non-malleable extractor. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 442–469. Springer, 2019.

[2] D. Aggarwal, I. Damgard, J. B. Nielsen, M. Obremski, E. Purwanto, J. Ribeiro, and M. Simkin. Stronger leakage-resilient and non-malleable secret-sharing schemes for general access structures. 2019. To appear.

[3] D. Aggarwal, A. Joux, A. Prakash, and M. Santha. A new public-key cryptosystem via mersenne numbers. In *Annual International Cryptology Conference*, pages 459–482. Springer, 2018.

[4] D. Aggarwal and P. Mukhopadhyay. Improved algorithms for the shortest vector problem and the closest vector problem in the infinity norm. In *29th International Symposium on Algorithms and Computation (ISAAC 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[5] D. Aggarwal, D. Nico, N. J. Buus, O. Maciej, and P. Erick. Continuous non-malleable codes in the 8-split-state model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 531–561. Springer, 2019.

[6] D. Aggarwal and M. Obremski. Inception makes non-malleable codes shorter as well! Cryptology ePrint Archive, Report 2019/399, 2019. `https://eprint.iacr.org/2019/399`.

[7] A. Anshu, I. Arad, and D. Gosset. Entanglement subvolume law for 2D frustration-free spin systems. *arXiv e-prints*, page arXiv:1905.11337, May 2019.

[8] A. Anshu, M. Berta, R. Jain, and M. Tomamichel. A minimax approach to one-shot entropy inequalities. Technical Report 1906.00333, arXiv, 2019.

[9] A. Anshu, M. Berta, R. Jain, and M. Tomamichel. Partially smoothed information measures. In *IEEE International Symposium on Information Theory (ISIT)*, 2019. Beyond I.I.D. in information theory (2018).

[10] A. Anshu, N. G. Boddu, and D. Touchette. Quantum log-approximate-rank conjecture is also false. In *60th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2019.

[11] A. Anshu, M.-H. Hsieh, and R. Jain. Noisy quantum state redistribution with promise and the alpha-bit. Technical Report 1803.03414, arXiv, 2018.

[12] A. Anshu, M.-H. Hsieh, and R. Jain. Quantifying resources in general resource theory with catalysts. *Phys. Rev. Lett.*, 121:190504, Nov 2018.

[13] A. Anshu and R. Jain. Efficient methods for one-shot quantum communication. Technical Report 1809.07056, arXiv, 2018.

[14] A. Anshu, R. Jain, and A. Streltsov. Quantum state redistribution with local coherence. Technical Report 1804.04915, arXiv, 2018.

[15] A. Anshu, R. Jain, and N. A. Warsi. Convex-split and hypothesis testing approach to one-shot quantum measurement compression and randomness extraction. *IEEE Transactions on Information Theory*, pages 1–1, 2019.

[16] A. Anshu, R. Jain, and N. A. Warsi. A hypothesis testing approach for communication over entanglement-assisted compound quantum channel. *IEEE Transactions on Information Theory*, 65(4):2623–2636, April 2019.

[17] A. Anshu, R. Jain, and N. A. Warsi. On the near-optimality of one-shot classical communication over quantum channels. *Journal of Mathematical Physics*, 60, Jan 2019.

[18] S. Arunachalam, S. Chakraborty, T. Lee, M. Paraashar, and R. de Wolf. Two new results about exact quantum learning. In *46th International Colloquium on Automata, Languages, and Programming*, 2019.

[19] E. Bairey, I. Arad, and N. H. Lindner. Learning a local hamiltonian from local measurements. *Phys. Rev. Lett.*, 122:020504, Jan 2019.

[20] T. Bannink, J. Briët, H. Buhrman, F. Labib, and T. Lee. Bounding quantum-classical separations for classes of nonlocal games. In *36th International Symposium on Theoretical Aspects of Computer Science, STACS 2019, March 13-16, 2019, Berlin, Germany*, pages 12:1–12:11, 2019.

[21] A. Belovs and A. Rosmanis. Quantum lower bounds for tripartite versions of the hidden shift and the set equality problems. In *13th Conference on the Theory of Quantum Computation, Communication and Cryptography*, pages 3:1–3:15, 2018.

[22] K. Bharti, M. Ray, and L.-C. Kwek. Non-classical correlations in n-cycle setting. *Entropy*, 21(2):134, Feb 2019.

[23] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L. C. Kwek. Robust self-testing of quantum systems via noncontextuality inequalities. *Physical Review Letters*, June 2019.

[24] F. L. Gall, H. Nishimura, and A. Rosmanis. Quantum advantage for the LOCAL model in distributed computing. In *36th International Symposium on Theoretical Aspects of Computer Science*, pages 49:1–49:14, 2019.

[25] D. Gavinsky. Quantum versus classical simultaneity in communication complexity. *IEEE Transactions on Information Theory*, 2019.

[26] D. Gavinsky, T. Lee, M. Santha, and S. Sanyal. A composition theorem for randomized query complexity via max conflict complexity. In *46th International Colloquium on Automata, Languages, and Programming*, 2019.

[27] S. Gharibian, M. Santha, J. Sikora, A. Sundaram, and J. Yirka. Quantum generalizations of the polynomial hierarchy with applications to qma(2). In *Proceedings of the 43rd International Symposium on Mathematical Foundations of Computer Science*, volume 58, pages 1–16, 2018.

[28] G. Ivanyos, P. Kutas, and L. Rónyai. Computing explicit isomorphisms with full matrix algebras over $\mathrm{F_q(x)}$. *Foundations of Computational Mathematics*, 18(2):381–397, 2018.

[29] G. Ivanyos, P. Kutas, and L. Rónyai. Explicit equivalence of quadratic forms over fq(t). *Finite Fields and Their Applications*, 55:33–63, 2019.

[30] G. Ivanyos and Y. Qiao. Algorithms based on *-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing. *SIAM Journal on Computing*, 48:926–963, 2019. Extended journal version of a conference paper from the previous report.

[31] G. Ivanyos, Y. Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Computational Complexity*, 27(4):561–593, 2018. Preprint reported in an earlier report.

[32] R. Jain, H. Klauck, S. Kundu, T. Lee, M. Santha, S. Sanyal, and J. Vihrovs. Quadratically tight

relations for randomized query complexity. In F. V. Fomin and V. V. Podolskii, editors, *Computer Science – Theory and Applications*, pages 207–219, Cham, 2018. Springer International Publishing.

[33] R. Jain, C. A. Miller, and Y. Shi. Parallel device-independent quantum key distribution. In *The 8th International Conference of Quantum Cryptography (QCrypt)*, 2018.

[34] T. Lee, M. Ray, and M. Santha. Strategies for Quantum Races. In A. Blum, editor, *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 51:1–51:21, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[35] N. Lindzey and A. Rosmanis. A tight lower bound for index erasure. (1902.07336), 2019.

[36] M. Obremski and M. Skorski. Complexity of estimating renyi entropy of markov chains. Cryptology ePrint Archive, Report 2019/766, 2019. `https://eprint.iacr.org/2019/766`.

[37] P. Rebentrost, B. Gupt, and T. R. Bromley. Photonic quantum algorithm for monte carlo integration. Technical Report 1809.02579, arXiv, 2018.

[38] P. Rebentrost and S. Lloyd. Quantum computational finance: quantum algorithm for portfolio optimization. Technical Report arXiv:1811.03975, arXiv, 2018.

[39] P. Rebentrost, M. Schuld, L. Wossnig, F. Petruccione, and S. Lloyd. Quantum gradient descent and newton's method for constrained polynomial optimization. *New Journal of Physics*, 2019. arXiv:1612.01789.

[40] F. Salek, A. Anshu, M.-H. Hsieh, R. Jain, and J. R. Fonollosa. One-shot capacity bounds on the simultaneous transmission of classical and quantum information. Technical Report 1809.07104, arXiv, 2018.

[41] L. Zhao, Z. Zhao, P. Rebentrost, and J. Fitzsimons. Compiling basic linear algebra subroutines for quantum computers. Technical Report 1902.10394, arXiv, 2019.