# Computer Science Project: Report 2019-2020

## I. INTRODUCTION

Our group has witnessed some changes over the last year. Marco Tomamichel has joined as a PI, but he will file a separate report. Naqueeb Warsi will move to Institute of Mathematical Sciences, India soon. Jianwei Li has moved to Royal Holloway, University of London. Ansis Rosmanis has moved to Nagoya University, Japan. Liming Zhao has joined the group as a Research Fellow. Jinge Bao has joined the group as a PhD student.

We have started some projects in collaboration with industry and secured a grant with MoE, and another with DSO.

## II. GROUP MEMBERS AND VISITORS

### A. Permanent group members

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

2. **Research Fellows**:
   Maciej Obremski
   Patrick Rebentrost
   Liming Zhao.

3. **Ph.D students**:
   Jinge Bao
   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 (6 months)
   Siyao Guo, New York University, Shanghai (1 month)
   Gábor Ivanyos, Hungarian Academy of Sciences (3 months)
   Antoine Joux, Université Pierre et Marie Curie (1 month)
   Iordanis Kerenidis, CNRS, Université Paris Diderot (1 months)
   Troy Lee, University of Technology Sydney (2 months)
   Serge Massar, Université Libre de Bruxelles (1 month)
   Pranab Sen, Tata Institute of Fundamental Research (1 month)
   Thomas Vidick, Caltech (1 month)
   Noah Stephens-Davidowitz, Cornell University (1 month).

2. **Temporary visitors**:
Luisa Siniscalchi, Wu Bujiao, Ronald Cramer, Joao Ribeiro, Quek Yihui, Anurag Anshu, Chen Yanlin, Christopher Williamson, Zhang Shengyu, Maciej Skorski.

## III. RESEARCH HIGHLIGHTS

### A. Algorithms and Complexity

1. Submodular functions are set functions mapping every subset of some ground set of size $n$ into the real numbers and satisfying the diminishing returns property. Submodular minimization is an important field in discrete optimization theory due to its relevance for various branches of mathematics, computer science and economics. The fastest strongly polynomial algorithm for exact minimization runs in time $O(n^3 \cdot EO + n^4)$ where  denotes the cost to evaluate the function on any set. For functions with range $[-1, 1]$, the best -additive approximation algorithm before this work run in time $O(n^{5/3}/^2 \cdot EO)$. In [HRRS19] we present a classical and a quantum algorithm for approximate submodular minimization. Our classical result improves on the above algorithm and runs in time $O(n^{3/2}/^2 \cdot EO)$. Our quantum algorithm is the first attempt to use quantum computing for submodular optimization. The algorithm runs in time $O(n^{5/4}/^{5/2} \cdot \log(1/) \cdot EO)$. The main ingredient of the quantum result is a new method for sampling with high probability $T$ independent elements from any discrete probability distribution of support size $n$ in time $O(\sqrt{Tn})$. Previous quantum algorithms for this problem were of complexity $O(T\sqrt{n})$.

2. In [IJS19] we investigated the classical and quantum complexity of computing discrete logarithms as well as the closely related computational and decisional Diffie-Hellman problems in certain black-box groups where the elements are encoded by an elementary abelian covering group and testing equality is given by and oracle. In contrast to Shor's celebrated result (which holds in the case of unique encoding), both computational problems remain hard even in the quntum query complexity model when the encoding group has at least rank two. Interestingly, the decisional Diffie-Hellman problem is even classically easy in the rank two case while from rank 3,already the quantum query complexity becomes exponential.

3. We continued to focus on quantum computing with applications to optimization and machine learning. One highlight is [HRR+20] which develops quantum algorithms for online learning in an oracular setting. We discuss quantum analogues of the famous Hedge algorithm by Freund/Schapire and also the Sparsitron, a machine learning algorithm based on the Hedge algorithm. The quantum algorithms inherit the provable guarantees from the classical algorithms and exhibit polynomial speedups. Our results also find application to the provable learning of Ising models and Markov Random Fields. Another highlight is [HBR19] on near-term quantum algorithms of solving linear systems of equations. Existing quantum algorithms have demonstrated the potential for significant speedups, but the required quantum resources are not immediately available on near-term quantum devices. In [HBR19], we investigate the use of variational algorithms and analyze their optimization landscapes. Such algorithms often suffer from barren plateau issues, hence we design a class of algorithms based on the classical combination of variational quantum states. Supported by the representation of the linear system on a so-called Ansatz tree, we exhibit provable guarantees for these algorithms.

4. In [ACKS20], we present new algorithms that improve the state-of-the-art for provable classical/quantum algorithms for SVP. We present the following results.

   (a) A new algorithm for SVP that provides a smooth tradeoff between time complexity and memory requirement. For any positive integer $4 \leq q \leq \sqrt{n}$, our algorithm takes $q^{11n+o(n)}$ time and requires $poly(n) \cdot q^{16n/q^2}$ memory. This tradeoff which ranges from enumeration ($q = \sqrt{n}$) to sieving ($q$ constant), is a consequence of a new time-memory tradeoff for Discrete Gaussian sampling above the smoothing parameter.

(b) A quantum algorithm that runs in time $2^{0.9532n+o(n)}$ and requires $2^{0.5n+o(n)}$ classical memory and $(n)$ qubits. This improves over the previously fastest classical (which is also the fastest quantum) algorithm that has a time and space complexity $2^{n+o(n)}$.

### B. Information Theory, Communication Complexity and Query Complexity

1. We worked on comparing quantum to classical communication. In [Gav20a], we presents a relational bipartite communication problem that has an efficient quantum simultaneous-messages protocol, but no efficient classical two-way protocol.

2. The adversary bound characterizes the quantum query complexity of any function and satisfies very nice properties like a perfect composition theorem. Belovs developed a modification of the adversary method that can be used to show lower bounds for relations as well, provided the relation is efficiently verifiable. Intuitively, this means that it is easy to verify that a particular output is valid for an input $x$. In [BL20] we show that this relational adversary bound is also an upper bound on the quantum query complexity of any relation. We further show a perfect composition theorem for the adversary bound of a relation composed with a function. Such a theorem was needed for a recent application by Alpers and de Wolf to lower bound the quantum query complexity of constructing a spectral sparsifier.

3. In [KL19] we investigate the problem of approximating inner products of the form $a^TBc$, where $a, c \in S^{n-1}$ and $B \in O_n$, in models of communication complexity and streaming algorithms. The worst meaningful approximation is to simply decide whether the product is 1 or -1, given the promise that it is either. We call that problem the $aBc$ problem. While very efficient streaming algorithms and one-way communication protocols are known for simple inner products (approximating $a^Tc$) we show that no efficient one-way protocols/streaming algorithms exist for the $aBc$ problem. In communication complexity we consider the 3-player number-in-hand model. We consider a setting where the players holding $B, c$ may confer over many rounds, while there is only one message to Alice.

   (a) In communication complexity $a^TBc$ can be approximated within additive error $\epsilon$ with communication $O(\sqrt{n}/\epsilon^2)$ by a one-way protocol Charlie to Bob to Alice.

   (b) The $aBc$ problem has a streaming algorithm that uses space $O(\sqrt{n}\log n)$

   (c) Any one-way communication protocol for $aBc$ needs communication at least $\Omega(n^{1/3})$, and we prove a tight results regarding a communication tradeoff: if Charlie and Bob communicate over many rounds such that Charlie communicates $o(n^{2/3})$ and Bob $o(n^{1/3})$, and then the transcript is sent to Alice, the error will be large.

   (d) To establish our lower bound we show concentration results for Rényi divergences under the event of restricting a density function on the sphere to a random equator and subsequently normalizing the restricted density function.

   (e) We show a strong concentration result for conditional Rényi divergences on bipartite systems for all $\alpha > 1$, which does not hold for $\alpha = 1$.

4. Smooth entropies are a tool for quantifying resource trade-offs in (quantum) information theory and cryptography. In typical bi-and multi-partite problems, however, some of the subsystems are often left unchanged and this is not reflected by the standard smoothing of information measures over a ball of close states. In [ABJT20] we propose to smooth instead only over a ball of close states which also have some of the reduced states on the relevant subsystems fixed. This partial smoothing of information measures naturally allows to give more refined characterizations of various information-theoretic problems in the one-shot setting. In particular, we immediately get asymptotic second-order characterizations for tasks such as privacy amplification against classical side information or classical state splitting. For quantum problems like state merging the general resource trade-off is tightly characterized by partially smoothed information measures as well.

5. One-shot information theory entertains a plethora of entropic quantities, such as the smooth max-divergence, hypothesis testing divergence, and information spectrum divergence, that characterize various operational tasks in quantum information theory and are used to analyze their asymptotic behavior. Tight inequalities between these quantities are thus of immediate interest. In [ABJT19], we use a minimax approach (appearing previously, for example, in the proofs of the quantum substate theorem), to simplify the quantum problem to a commutative one, which allows us to derive such inequalities. Our derivations are conceptually different from previous arguments and in some cases lead to tighter relations. We hope that the approach discussed here can lead to progress in open problems in quantum Shannon theory and exemplify this by applying it to a simple case of the joint smoothing problem.

### C. Coding Theory and Cryptography

1. We have been working on various problems regarding non-malleability and leakage resilience, but perhaps the most interesting results were achieved in the field of randomness extraction. In [AOR+20b], we discuss various scenario where we have access to multiple sources of randomness, however some of them might be malicious. The honest sources produce samples that are independent of each other and have some entropy, while malicious sources produce samples arbitrarily correlated with all previous samples (SHELA -Somewhere Honestly Entropic LookAhead- sources). This kind of sources are quite natural in cryptography and appear f.e. in blockchain. Authors discuss different scenarios and show that while extraction is not possible from such sources, one can still hope to obtain Somewhere Random sources (source consisting of multiple blocks, where some of the blocks are uniform, but we don't know which). This starts the study of somewhere-extraction (extractor that produces somewhere random output instead of uniform output). Authors show multiple applications and some bounds highlighting the advantages of SHELA sources over the general weak sources. In the follow up paper [AGO+20] authors propose a new framework for proving lower bounds both for Extractors and Somewhere Extractors. In particular authors show that Somewhere Extractors follow similar bounds to extractors altho with slightly better constants ( $\log(1/\epsilon)$ instead of $2\log(1/\epsilon)$ ). Also authors show how this new framework can be used to obtain very simple and short RT bounds proof.

2. In [MS20], we show how to generalize lattice reduction algorithms to module lattices in order to reduce $\gamma$-approximate ModuleSVP over module lattices with rank $k \geq 2$ to $\gamma'$-approximate ModuleSVP over module lattices with rank $2 \leq \beta \leq k$. To do so, we modify the celebrated slide-reduction algorithm of Gama and Nguyen to work with module filtrations, a higher-dimensional analogue of the ($\mathbb{Z}$-)basis of a lattice. The particular value of $\gamma$ that we achieve depends on the underlying number field $K$, the ring $R \subset K$, and the embedding (as well as, of course, $k$ and $\beta$). However, for reasonable choices of these parameters, the approximation factor that we achieve is surprisingly close to the one achieved by "plain" lattice reduction algorithms, which require an arbitrary SVP oracle in the same dimension. In other words, we show that ModuleSVP oracles are nearly as useful as SVP oracles for solving approximate ModuleSVP in higher dimensions. Our result generalizes the recent independent result of Lee, Pellet-Mary, Stehle, and Wallet, which works in the important special case when $\beta = 2$ and $R = \mathcal{O}_K$ is the ring of integers of $K$ under the canonical embedding. Indeed, at a high level our reduction can be thought of as a generalization of theirs in roughly the same way that slide reduction generalizes LLL reduction.

3. Device-independent cryptography aims to do cryptographic tasks in the scenario where the honest parties involved don't trust their own (quantum) devices. Device-independent quantum protocols were previously known for tasks such as key distribution, bit commitment and coin flipping. In [KST20], we give the first device-independent quantum protocol for the cryptographic primitive XOR oblivious transfer, which is a variant of the well-known oblivious transfer. Our protocol is based on the rigidity property of the magic square nonlocal game and is provably more secure than any classical protocol. Work is currently ongoing

to show reductions from XOR oblivious transfer to oblivious transfer, and using our bounds on XOR oblivious transfer to prove bounds on oblivious transfer.

4. In [ALNS20], we show to generalize Gama and Nguyen's slide reduction algorithm [STOC '08] for solving the approximate Shortest Vector Problem over lattices (SVP). As a result, we show the fastest provably correct algorithm for $\delta$-approximate SVP for all approximation factors $n^{1/2+} \leq \delta \leq n^{O(1)}$. This is the range of approximation factors most relevant for cryptography.

## IV. TEACHING AND OUTREACH

### A. Teaching

1. Divesh Aggarwal: *Design and Analysis of Algorithms* (CS3230), NUS, Semester 1 and Semester 4, 2019-20.

2. Hartmut Klauck: *Algorithms and Theory of Computing*, MAS 714, Semester 1, 2019-20 at NTU.

3. Rahul Jain: *Quantum Computing* (CS4268), NUS, Semester 1, 2019-20.

4. Srijita Kundu: Teaching assistant for *Quantum Computing* (CS4268), NUS, Semester 1, 2019-20.

5. Naresh Boddu: Teaching assistant for *Quantum Computing* (CS4268), NUS, Semester 1, 2019-20.

### B. Outreach

1. Patrick Rebentrost: Plenary presentation to Baidu employees on "Steps towards Quantum AI" (October 2019).

## V. FINANCE AND EXPENDITURE

Our expenditure last year has been at the usual rate (around 600 K SGD per year) and we have some fund balance that will carry over to the next academic year.

In addition we have a *VanQuTe* grant (amount 144 K, period 2019-2021)), a grant from Baidu (amount 180 K SGD, period April 2019 - January 2020), a grant from MOE (amount 303 K, Period 2020-2022), and a grant from DSO (amount 125K, Period 2020-2022). Please refer to section VI B for details.

## VI. APPENDIX

### A. Invited and contributed talks

1. Miklos Santha

   Baidu Quantum Centre, 30 October 2019, invited talk
   7th French - Israeli FILOFOCS workshop, Tel Aviv, Israel, 26-28 November 2019, invited talk

2. Patrick Rebentrost

   Invited talk at "Quantum techniques for machine learning" (QTML), Daejeon, Korea. October 2019.

   NTU lecture for masters students on "Quantum computing and financial applications". January 2020.

3. Rahul Jain

   *Workshop on Sensitivity, Query Complexity, Communication Complexity and Fourier Analysis of Boolean Function*, 19-21 February 2020, Indian Statistical Institute (ISI), Kolkata, India.

4. Srijita Kundu

   *Quantum Innovators in Computer Science & Mathematics Workshop*, 21-24 October 2019, Institute for Quantum Computing (IQC), University of Waterloo, Waterloo, Canada.

   *15th Conference on the Theory of Quantum Computation, Communication & Cryptography*, 9-12 June 2020, Online.

5. Naresh Boddu:

   *NUS Computer Science Research Week 2019*, 5-9 August 2019, NUS, Singapore.

   *60th Annual IEEE Symposium onFoundations of Computer Science*, 9-12 November 2019, Baltimore, Maryland.Boddu (joint talk): *23rd Annual Conference on Quantum Information Processing*, 6-10 January 2020, Shenzhen, China.

### B. Grants and Awards

1. Divesh Aggarwal is the main PI for MOE-funded Tier 2 project, titled "Foundations of quantum-safe cryptography" *MOE2019-T2-1-145*. Amount 303,000 SGD. Period 2020-2022.
2. Divesh Aggarwal is the main PI for DSO-funded project, titled "Design and Analysis of Lattice PQC Encryption scheme". *DSOCL19177* Amount 125,000 SGD. Period 2020-2022.
3. Rahul Jain is a co-PI for the *NRF2017-NRF-ANR004 VanQuTe* grant, a joint grant between Singapore and French institutes. Amount 144,000 SGD. Period 2019-2021.
4. Miklos Santha is Main PI for the Research Collaboration Agreement between Baidu and NUS on "Quantum algorithms for search, optimization and algebraic problems" from 15 April 2019 till 15 January 2020. Amount of the grant: 180,000 SGD.

### C. Professional activities

1. Divesh Aggarwal
   (a) served on the PC of EUROCRYPT 2020, SCN 2020 and ANTS 2020.
   (b) Member, Academic Committee (CQT).
   (c) Member, Graduate Students Admission Committee (School of Computing, NUS).
2. Miklos Santha
   (a) Member of the steering committee of Fundamentals of Computation Theory and the OIST Cyber-Security Center

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

(c) member of the PC of Quantum Technology International Conference, Paris, 2020

3. Troy Lee

(a) Joined steering committee of QIP.

(b) Jury member for the Airbus Quantum Computing Challenge.

4. Rahul Jain

(a) Member, Program Committee, QCRYPT 2020 and STOC 2020.

(b) Editor, *Journal of Computer and System Sciences* (JCSS).

(c) Guest Editor, *IEEE Journal on Selected Areas in Information Theory* (JSAIT), Special Issue on Quantum Information Science, 2020.

(d) Chair, Mid-Term Advisory Report (MTAR) Committee for Promotion and Tenure(SoC, NUS), 2019.

(e) Member, IT Committee (CQT), Academic Committee (CQT).

## VII. PUBLICATIONS AND PREPRINTS


[ABGS19] Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. Fine-grained hardness of cvp (p)—everything that we can prove (and nothing else). *arXiv preprint arXiv:1911.02440*, 2019.

[ABJT19] Anurag Anshu, Mario Berta, Rahul Jain, and Marco Tomamichel. A minimax approach to one-shot entropy inequalities. *Journal of Mathematical Physics*, 60(12):122201, 2019.

[ABJT20] Anurag Anshu, Mario Berta, Rahul Jain, and Marco Tomamichel. Partially smoothed information measures. *IEEE Transactions on Information Theory*, pages 1–1, 2020.

[ABT19] Anurag Anshu, Naresh Goud Boddu, and Dave Touchette. Quantum Log-Approximate-Rank Conjecture is also False. In *Proceedings of the 60th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2019.

[ACKS20] Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, and Yixin Shen. Improved (provable) algorithms for the shortest vector problem via bounded distance decoding. *arXiv preprint arXiv:2002.07955*, 2020.

[ADN+19] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, Joao Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In *CRYPTO*, 2019.

[AGO+20] Divesh Aggarwal, Siyao Guo, Maciej Obremski, Joao Ribeiro, and Noah Stephens-Davidowitz. Extractor lower bounds, revisited. In *RANDOM*, 2020.

[ALNS20] Divesh Aggarwal, Jianwei Li, Phong Q Nguyen, and Noah Stephens-Davidowitz. Slide reduction, revisited—filling the gaps in svp approximation. In *CRYPTO*, 2020.

[AO19] Divesh Aggarwal and Maciej Obremski. A constant-rate non-malleable code in the split-state model. *Cryptology ePrint Archive Report 2019/1299*, 2019.

[AOR+20a] Divesh Aggarwal, Maciej Obremski, Joao Ribeiro, Mark Simkin, and Luisa Siniscalchi. Computational and information-theoretic two-source (non-malleable) extractors. Technical Report Report 2020/259, Cryptology ePrint Archive, 2020.

[AOR+20b] Divesh Aggarwal, Maciej Obremski, João Ribeiro, Luisa Siniscalchi, and Ivan Visconti. How to extract useful randomness from unreliable sources. In *Eurocrypt 2020*, 2020.

[AS19] Divesh Aggarwal and Noah Stephens-Davidowitz. An improved constant in banaszczyk's transference theorem. *arXiv preprint arXiv:1907.09020*, 2019.

[BFO+20] Gianluca Brian, Antonio Faonio, Maciej Obremski, Mark Simkin, and Daniele Venturi. Non-malleable secret sharing against bounded joint-tampering attacks in the plain model. In *Crypto 2020*, 2020.

[BL20] Aleksandrs Belovs and Troy Lee. The quantum query complexity of composition with a relation. Technical Report arXiv:2004.06439, arXiv, 2020.

[Gav19] D. Gavinsky. Quantum versus classical simultaneity in communication complexity. *IEEE Transactions on Information Theory*, 2019.

[Gav20a] D. Gavinsky. Bare quantum simultaneity versus classical interactivity in communication complexity. In *STOC*, 2020.

[Gav20b] D. Gavinsky. Entangled simultaneity versus classical interactivity in communication complexity. *IEEE Transactions on Information Theory*, 2020.

[GP20] D. Gavinsky and P. Pudlak. Santha-vazirani sources, deterministic condensers and very strong extractors. *Theory of Computing Systems*, 2020.

[HBR19] Hsin-Yuan Huang, Kishor Bharti, and Patrick Rebentrost. Near-term quantum algorithms for linear systems of equations. Technical Report 1909.07344, arXiv, 2019.

[HRR+20] Yassine Hamoudi, Maharshi Ray, Patrick Rebentrost, Miklos Santha, Xin Wang, and Siyi Yang. Quantum algorithms for hedging and the sparsitron. Technical Report 2002.06003, arXiv, 2020.

[HRRS19] Y Hamoudi, P Rebentrost, A Rosmanis, and M Santha. Quantum and classical algorithms for approximate submodular function minimization. *Quantum Information and Computation*, 19:1325–1349, 2019.

[IJS19] G. Ivanyos, A. Joux, and M. Santha. Discrete logarithm and diffie-hellman problems in identity black-box groups. Technical Report 1911.01662 [quant-ph], arXiv, 2019.

[JKK+20] R Jain, H Klauck, S Kundu, T Lee, M Santha, S Sanyal, and J Vihrovs. Quadratically tight relations for randomized query complexity. *Theory of Computing Systems*, 64:101–119, 2020.

[KL18] H. Klauck and D. Lim. The power of one clean qubit in communication complexity. Technical Report CoRR/1807.07762, arXiv, 2018.

[KL19] H. Klauck and D. Lim. The abc problem and equator sampling renyi divergences. Technical Report CoRR/1912.11275, arXiv, 2019.

[KM19] Upendra Kapshikar and Ayan Mahalanobis. The Niederreiter cryptosystem and Quasi-Cyclic codes. *CoRR*, abs/1911.00661, 2019.

[KST20] Srijita Kundu, Jamie Sikora, and Ernest Y.-Z. Tan. A device-independent protocol for XOR oblivious transfer. In *Proceedings of the 15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, 2020. To appear.

[LBP+20] Seth Lloyd, Samuel Bosch, Giacomo De Palma, Bobak Kiani, Zi-Wen Liu, Milad Marvian, Patrick Rebentrost, and David M. Arvidsson-Shukur. Quantum polar decomposition algorithm. Technical Report 2006.00841, arXiv, 2020.

[MS20] T. Mukherjee and N. Stephens-Davidowitz. Lattice reduction for modules, or how to reduce modulesvp to modulesvp. In *CRYPTO*, 2020.

[OS20] Maciej Obremski and Maciej Skorski. Complexity of estimating renyi entropy of markov chains. In *International Symposium on Information Theory, ISIT 2020*, 2020.

[YQ20] Patrick Rebentrost Yihui Quek, Clement Canonne. Robust quantum minimum finding with an application to hypothesis selection. Technical Report 2003.11777, arXiv, 2020.