Computer Science Project: Report 2016-2017

I. INTRODUCTION

Divesh Aggarwal has joined the School of Computing at NUS as Assistant Professor and CQT as PI in August 2016. He is now a member of the CS group in CQT. With his arrival the group has started a new research axis, quantum safe cryptography. Post-quantum cryptography is concerned with the design and the evaluation of cryptographic systems which are resistant even to quantum attacks. The group has already expertise in the design and analysis of efficient quantum algorithms whose potential use for testing the security of various cryptographic systems is also investigated. Complementing that, the new research effort is specifically targeted towards the conception of new cryptosystems which remain secure against quantum attacks, as well as the study of the theoretical and algorithmic foundations of these systems. Divesh's scientific report is included in this document.

Joe Fitzsimons, Assistant Professor since 2013 at the Singapore University of Technology and Design, has also joined CQT as PI in August 2016. Joe's research area concerns the verification of quantum computation, and he has an NRF Fellowship on that subject. While Joe has various collaborations with the CS group, he had already his research team when he joined CQT and his scientific report is filed separately.

Our group visitors program was significantly extended during the last year. Antoine Joux from the Université Pierre et Marie Curie and Hoeteck Wee from the CNRS, Ecole Normale Supérieure will contribute to the new research on quantum safe cryptography. Itai Arad from Technion was previously Senior Research Fellow in CQT, during his visits he will continue to work on Hamiltonian complexity. Serge Massar from the FNRS, Université Libre de Bruxelles has double competence in quantum information theory and theoretical computer science, he is expected to collaborate with both CS and Theoretical Pysics PI's in CQT.

As in the previous years, Troy Lee's NRF Fellowship on *Quantum query complexity, communication complexity, and semidefinite programming* is handled by NTU with a formal project agreement between NTU and CQT.

In October 2016 we have organized a workshop on "Quantum Safe Cryptography" and in March 2017 a workshop on "Post Quantum-Cryptanalysis". Between 4 and 8 September 2017 we have hosted the "17th Asian Quantum Information Science Conference". AQIS is probably the second biggest general conference in quantum computing and information theory after QIP, the number of participants was above 100. To celebrate the 10th anniversary of CQT, we will organize a workshop on "Quantum Algorithms and Complexity Theory" between 26 February and 2 March 2018.

II. GROUP MEMBERS AND VISITORS

A. Permanent group members

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

2. **Research Fellows**:
   Han-Hsuan Lin
   Anupam Prakash
   Ansis Rosmanis
   Swagato Sanyal
   Jamie Sikora (until June 2017)

Antonios Varvitsiotis
Naqueeb Warsi
Zhaohui Wei (until September 2017).

3. **Ph.D students**: Anurag Anshu
Naresh Goud Buddu
Priyanka Mukhopadhyay
Supartha Podder (graduated in September 2016)
Erick Purwanto
Maharshi Ray
Aarthi Sundaram (graduated in August 2017)
Siyi Yang.

4. **Research Assistant**: Varun Raj.

B. Visitors

1. **Regular Visiting Researchers**:
Itai Arad, Technion (2 months, started in 2017)
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, started in 2017)
Iordanis Kerenidis, CNRS, Université Paris Diderot (2 months)
Serge Massar, FNRS, Université Libre de Bruxelles (1 month, started in 2017)
Thomas Vidick, Caltech (1 month)
Hoeteck Wee, CNRS, Ecole Normale Supérieure (1 month, started in 2016).

2. **Interns**:
Yupan Liu (Zhejiang University, Hangzhou, 1 July 2016 - 3 September 2016),
Naresh Goud Boddu, (IIT Madras, 03 January 2017 - 02 April 2017),
Yassine Hamidou (ENS Lyon, 1 April 2017 - 30 June 2017),
Mahak Sarin (Indian Institute of Technology, Ropar, 22 May 2017 - 21 July 2017),
Tomas Vyskocil (Rutgers University, 1 June 2017 - 31 August 2017).

3. **Temporary visitors**:
Cedric Yen-Yu Lin (QuICS, University of Maryland, 5 December 2016 - 17 December 2016)
Edward Fahri (MIT, 6 December 16 - 9 December 16)
Jevgenijs Vihrovs (University of Latvia, 1 October 2016 - 31 December 2016)
Dominique Unruh (University of Tartu, 31 Jan 2017 - 3 February 2017)
Kai-Min Chung (Academia Sinica, Taipei, 20 February 2017 - 24 February 2017)
Ronald Cramer (CWI Amsterdam, 22 February 2017 - 22 March 2017 and 7 October 2017 - 7 November 2017)
Michel de Rougemont (Université Paris Diderot, France, 24 April 2017 - 28 April 2017)
Jingbo Wang (University of Western Australia, 3 September 2017 - 29 September 2017)
Henry Yuen (UC Berkeley, 11 September 2017 - 23 September 2017)
Gavin Brennen (Macquarie University, Sydney, 18 September 2017 - 22 September 2017)
Marco Tomamichel (U. of Technology Sydney, 18 September 2017 - 22 September 2017)
Benny Chor (Tel Aviv University, 27 October 2017 - 30 October 2017).

III. RESEARCH HIGHLIGHTS

A. Algorithms and Complexity

1. A linear system solver is a powerful tool in machine learning, since it can be leveraged to solve optimization problems using iterative methods like gradient descent or the interior point method. It remains an open question whether quantum linear system solvers can be used similarly. In [51], we provide the first quantum method for performing gradient descent for cases where the gradient is an affine function. Performing n steps of the quantum gradient descent requires time $O(Cn)$, where C is the cost of performing quantumly one step of the gradient descent, which can be exponentially smaller than the cost of performing the step classically. We provide two applications of our quantum gradient descent algorithm: first, for solving positive semidefinite linear systems, and, second, for performing stochastic gradient descent for the weighted least squares problem. We also provide an improved quantum linear system solver that provides exponential savings for large families of matrices (even dense), for example for matrices with rank poly-logarithmic in matrix dimensions.

2. The Polynomial Parity Argument complexity class PPA consists of NP-search problems which are reducible to the parity principle in undirected graphs. It contains a wide variety of interesting problems from graph theory, combinatorics, algebra and number theory, but only a few of these are known to be complete in the class. Before this work, the known complete problems were all discretizations or combinatorial analogues of topological fixed point theorems. In [31] we prove the PPA-completeness of two problems of radically different style. They are PPA-Circuit CNSS and PPA-Circuit Chevalley, related respectively to the Combinatorial Nullstellensatz and to the Chevalley-Warning Theorem over the two elements field. The input of these problems contain PPA-circuits which are arithmetic circuits with special symmetric properties that assure that the polynomials computed by them have always an even number of zeros. In the proof of the result we relate the multilinear degree of the polynomials to the parity of the maximal parse subcircuits that compute monomials with maximal multilinear degree, and we show that the maximal parse subcircuits of a PPA-circuit can be paired in polynomial time.

3. In [45] we applied techniques from the theory of $*$-algebras (algebras with involutions) to certain computational problems. One of them is simultaneous isometry of tuples of quadratic forms. Over a finite base field we gave a randomized polynomial time solution to this problem. Our result has interesting applications including isomorphism of certain nilpotent groups of class two (these are thought to be the main obstacles to testing isomorphisms of groups) as well as solving the problem called IP1S (isomorphisms of polynomials with one secret), that an authentication scheme proposed by Patarin is based on. We also considered the problem of simultaneously transforming tuples of matrices to (skew-)symmetric matrices by mulltiplications from the left and from the right. This task belongs to the famous class of polynomial identity testing for which randomized polynomial algorithms are available but existence of efficient deterministic methods is a major open question in algebraic complexity theory. For the specific problem our $*$-algebra method leads to a deterministic polynomial time solution. Deterministic constructions of irreducible polynomials over finite fields of large characteristic is another major open problem. In [33] we made a step towards a possible solution: we devised a deterministic polynomial time algorithm that, given a polynomial which is a product of m irreducible polynomials of prime degree r not dividing m, constructs an irreducible polynomial of degree r.

4. A long standing problem in the theory of tensor-network is the contraction of PEPS tensor-networks. These are 2D tensor-networks that naturally satisfy the area-law and are therefore frequently used to model the ground states of 2D systems. However, in order to use these tensor networks to evaluate the expectation values of local operators, one need to contract the resultant 2D tensor networks. Such operations are generally known to be #P-hard, and so one usually resorts to approximations. Such approximations, while physically motivated,

are nevertheless uncontrolled, and sometimes result in biased results. In a recent work [29] [a local set of constraints for the reduced density matrices of local Hamiltonian eigenstates we raised the possibility that while the contraction of general PEPS tensor-network is #P-hard, the contraction of such tensor-networks that describe the ground state of gapped local Hamiltonian might be much easier, hopefully in P. Indeed, one might be able use the extra structure of the local Hamiltonian to facilitate the contraction. We gave two general frameworks for such a contraction, and checked them numerically. In the current manuscript we continue to explore one of these methods by checking it against exactly solveable models such the the transverse Ising model, the XY model and Kitaev's honeycomb model. We prove semi-analytically that in these models our method is works. In addition we study the general conditions under which the method is excepted to work, thereby identifying a large family of models for which the contraction of PEPS can be done efficiently.

B. Interaction, Games

1. In [55] we introduce a two-player nonlocal game, called the (G, H)-isomorphism game, where classical players can win with certainty if and only if the graphs G and H are isomorphic. We then define the notions of quantum and no-signaling isomorphism, by considering perfect quantum and no-signaling strategies for the (G, H)-isomorphism game, respectively. We prove that no-signaling isomorphism coincides with the well-studied notion of fractional isomorphism, thus giving the latter an operational interpretation. Second, we show that quantum isomorphism is equivalent to the feasibility of two polynomial systems in non-commuting variables, obtained by relaxing the standard integer programming formulations for graph isomorphism to Hermitian variables. On the basis of this correspondence, we identify quantum isomorphic graphs that are not isomorphic.

2. The study of interaction between quantum players is essential to understanding many tasks in quantum computing and information theory. In [43] we studied the notion of quantum strategies, which is a description of the actions one player executes in a two-player quantum interaction. In particular, we studied the extent one party can flip-flop between strategies, in an attempt to cheat the other player. We apply this to several tasks in quantum cryptography where the ability to switch between strategies reveals cheating strategies in highly-interactive protocols. When combining our work with an older paper of Gutoski, we provide impossibility proofs which say that even in the quantum world, certain cryptographic tasks are impossible.

3. 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 (STOC'09) 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 [2] 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 (FOCS'12), 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.

4. A device-independent dimension test for a Bell experiment aims to estimate the underlying Hilbert space dimension that is required to produce given measurement statistical data without any other assumptions concerning the quantum apparatus. Previous work deals with the two-party version of this problem, and multipartite cases have never been considered before. In [64], we propose a very general and robust approach to test the dimension of any subsystem in a multiparty Bell experiment. Our dimension test stems from the study of a new multiparty scenario which we call prepare-and-distribute. Through specific examples,

we show that our test results can be tight. Furthermore, we compare the performance of our test to results based on known bipartite tests, and witness remarkable advantage, which indicates that our test is of a true multiparty nature. We conclude by pointing out that with some partial information about the quantum states involved in the experiment, it is possible to learn other interesting properties beyond dimension.

C. Communication Complexity, Query Complexity and other aspects of Communication

1. In a series of works [22–26], we have developed a unified approach to study one-shot quantum Shannon theory. Quantum Shannon theory hosts a wide variety of scenarios, such as the point to point quantum channel coding with and without entanglement, quantum channels in network scenarios, quantum source compression in both two-party and distributed scenarios and classical-quantum scenarios. Previous literature used many unrelated techniques to find the achievable communication in all of the above. Our approach uses two techniques of convex-split [14] and position-based decoding [26]. It has consequences in all of the above tasks, and gives near-optimal answers in some important cases which was not known previously (point to point quantum channel coding and quantum state merging). In some cases, our results improve upon previous works (such as for quantum state redistribution). We have also found implications in the well studied quantum resource theory [18].

2. A popular direction of research in complexity theory is understanding the complexity of composition of two functions in terms of the complexities of the original functions. This question has been studied in the past for various measures of complexities: approximate degree, conical junta degree, query complexity, etc. For all natural complexity measures, the complexity of the composed function is bounded above by the product of the complexities of the original functions. A natural question is if this upper bound is tight; is it true that the complexity of a composed function is asymptotically bounded below by the product of the complexities of the original functions? We make progress in answering this question when the complexity measure is the bounded-error randomized query complexity. In the work [16], we show that the bounded-error randomized query complexity of a composed function for constant error is asymptotically bounded below by the product of the bounded-error randomized query complexity of the outer function for constant error and the bounded-error randomized query complexity of the inner function for error $\frac{1}{2} - \frac{1}{\text{poly}(n)}$, where n is the number of inputs to the outer function. Our result, coupled with an XOR lemma by Andrew Drucker, implies that if an XOR function on $\Theta(\log n)$ inputs is introduced between the inner and the outer function, the direct upper bound described above is asymptotically optimal.

3. One of the best lower bound methods for the quantum communication complexity of a function H (with or without shared entanglement) is the logarithm of the approximate rank of the communication matrix of H. This measure is essentially equivalent to the approximate γ_2 norm and generalized discrepancy, and subsumes several other lower bounds. All known lower bounds on quantum communication complexity in the general unbounded-round model can be shown via the logarithm of approximate rank, and it was an open problem to give any separation at all between quantum communication complexity and the logarithm of the approximate rank. In the work [13], we provide the first such separation: We exhibit a total function H with quantum communication complexity almost quadratically larger than the logarithm of its approximate rank. We construct H using the communication lookup function framework of Anshu et al. (FOCS 2016) based on the cheat sheet framework of Aaronson et al. (STOC 2016). From a starting function F, this framework defines a new function $H = F_G$. Our main technical result is a lower bound on the quantum communication complexity of F_G in terms of the discrepancy of F, which we do via quantum information theoretic arguments. We show the upper bound on the approximate rank of F_G by relating it to the Boolean circuit size of the starting function F.

4. In the work [19] we present the following quantum compression protocol $\mathcal{P}$: Let ρ, σ be quantum states such that $S(\rho||\sigma) = Tr(\rho \log \rho - \rho \log \sigma)$, the relative entropy between ρ

and σ, is finite. Alice gets to know the eigen-decomposition of ρ. Bob gets to know the eigen-decomposition of σ. Both Alice and Bob know $S(\rho||\sigma)$ and an error parameter ϵ. Alice and Bob use shared entanglement and after communication of $O((S(\rho||\sigma)+1)/\epsilon^4)$ bits from Alice to Bob, Bob ends up with a quantum state ρ' such that $F(\rho,\rho') \geq 1-5\epsilon$, where F represents fidelity. This result can be considered as a non-commutative generalization of a result due to Braverman and Rao [2011] where they considered the special case when ρ and σ are classical probability distributions (or commute with each other) and use shared randomness instead of shared entanglement. We use $\mathcal{P}$ to obtain an alternate proof of a direct-sum result for entanglement assisted quantum one-way communication complexity for all relations, which was first shown by Jain, Radhakrishnan and Sen [2005,2008]. We also present a variant of protocol $\mathcal{P}$ in which Bob has some side information about the state with Alice. We show that in such a case, the amount of communication can be further reduced, based on the side information that Bob has. Our second result provides a quantum analogue of the widely used classical correlated-sampling protocol. For example, Holenstein [2007] used the classical correlated-sampling protocol in his proof of a parallel-repetition theorem for two-player one-round games.

5. The quantum query algorithm is a computational model that facilitates our understanding of the computational power and limitations of quantum computers. The quantum query complexity of a function is the number of times an algorithm has to access an input in order to compute the value of the function on this input. In theory, this complexity is completely characterised by the quantum adversary method, yet it is often not known how to use this method effectively. We showed how to apply the adversary method to obtain optimal lower bounds on the quantum query complexity of the collision and set equality problems, two basic functions of great interest in quantum computing. We subsequently simplified our results [32], requiring less technical knowledge for the application.

6. In [38] we present a bipartite partial function, whose communication complexity is $O((\log n)^2)$ in the model of quantum simultaneous message passing and $\tilde{\Omega}(\sqrt{n})$ in the model of randomised simultaneous message passing. In fact, the function has a poly-logarithmic protocol even in the (restricted) model of quantum simultaneous message passing without shared randomness, thus witnessing the possibility of qualitative advantage of this model over randomised simultaneous message passing with shared randomness. This can be interpreted as the strongest known – as of today – example of "super-classical" capabilities of the weakest studied model of quantum communication.

D. Quantum safe cryptography

1. In the last two decades, many cryptographic primitives have been constructed whose security is based on the (worst-case) hardness of the shortest vector problem (SVP) in lattices or closely related lattice problems. While most of these applications rely on approximate variants of SVP with rather large approximation factors (e.g., approximation factors that are polynomial in n for most cryptographic constructions, where n is the rank of the lattice), the best known algorithms for the approximate variant of SVP use an algorithm for exact SVP in lower dimensions as a subroutine. So, the complexity of the exact problem is of particular interest. While NP-hardness of SVP is well studied, such hardness proofs tell us very little about the *quantitative* or *fine-grained* complexity of SVP. E.g., does the fastest algorithm for SVP run in time at least, say, $2^{n/5}$, or is there an algorithm that runs in time $2^{n/20}$ or even $2^{\sqrt{n}}$? The above hardness results cannot distinguish between these cases, but we certainly need to be confident in our answers to such questions if we plan to base the security of widespread cryptosystems on these answers.

   Our main results in[10] are the following: We give an explicit constant $C_p > 0$ for $p > p_0 \approx 2.14$ such that, under (randomized) strong exponential time hypothesis, there is no algorithm for SVP in the ℓ_p norm on n-dimensional lattices that runs in time better than $2^{n/C_p}$. For any $p > 2$, we prove that there is no $2^{o(n)}$-time algorithm for SVP in the ℓ_p norm unless

(randomized) Gap Exponential time Hypothesis (Gap-ETH) fails. We establish that there is no $2^{o(n)}$-time algorithm for SVP in the ℓ_2 norm unless either (non-uniform) Gap-ETH is false or the lattice kissing number is $2^{o(n)}$.

2. In [8] we modify the randomized sieving algorithm of Ajtai, Kumar and Sivakumar [2001,2002] to solve Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) in the ℓ_∞ norm, that results in substantial quantitative improvement over prior results. We make a simple but powerful observation that for the special case of the ℓ_∞ norm, if we partition the ambient space $[-R, R]^n$ into $([-R, -R+\gamma), [-R+\gamma, -R+2\gamma), \ldots)^n$, then it is easy to see that each such partition will contain at most one centre. Given a vector in S we can find its partition by checking the interval in which each co-ordinate belongs and then check whether this partition contains a centre. This drastically improves the running time for the sieving procedure in the SVP algorithm from $|S| \cdot |C|$ to $|S| \cdot n$. We then use the same idea to obtain significantly faster approximation algorithms for both SVP and CVP. Along the way, we optimize several steps specialized to the case of ℓ_∞ norm in the analysis of these algorithms. We also show that the heuristic sieving algorithms of Nguyen and Vidick [2008] and Wang et. al. [2011] can also be analysed in the ℓ_∞ norm. The main technical contribution for analyzing the space and time complexity is to calculate the expected volume of intersection of a unit ball centred at origin and another ball of a different radius centred at a uniformly random point on the boundary of the unit ball.

3. Predicate encryption is a novel paradigm for encrypting data that enables fine-grained access control and selective computation, as is necessary to protect big, complex data. In [34] we provide new constructions of predicate encryption schemes for the class of circuits whose security relies on the conjectured intractability of lattice problems, which we believe to also be resilient to quantum attacks.

IV. TEACHING AND OUTREACH

A. Teaching

1. Divesh Aggarwal course on *Introduction to Information Theory* (CS3236), NUS, Spring 2017.
2. Rahul Jain course on *Advanced Algorithms* (CS 6234), NUS, Spring 2017.
3. Hartmut Klauck course on *Computational Economics* (MH4320), NTU, Fall 2016; course on *Discrete Mathematics* (MH 1301), NTU, Spring 2017, course on *Computational Economics* (MH4320), NTU, Fall 2017.
4. Troy Lee course on *Linear Algebra I* (MH1200) NTU, Fall 2016 and Fall 2017
5. Jamie Sikora course on *Quantum Information and Cryptography* (QT5201L) NUS, Fall 2016
6. Antonios Varvitsiotis course on *Convex Optimization and Quantum Foundations* (QT5201N), NUS, Spring 2017.

B. Outreach

1. CQT has offered a five days Summer School titled "Generation Q Camp" in June 2017 in quantum technologies and cryptography for high-school students. Students have studied advanced concepts in mathematics, quantum physics, classical and quantum cryptography, and have seen experiments demonstrating quantum phenomena. From the CS group Anurag Anshu , Srijita Kundu, Anupam Prakash, Maharshi Ray, Jamie Sikora (main organizer) and Aarthi Sundaram have participated in the school.
2. Rahul Jain participated in NUS outreach events for students and parents in 2017.
3. Anurag Anshu volunteered at Art and Science Museum for Quantum Shorts Films Screening, February 2017.
4. Divesh Aggarwal gave a tutorial talk on post-quantum cryptography for employees of Infineon, May 2017.
5. Antonios Varvitsiotis supervised a research project on the Traveling Salesman Problem for high school students from Singapore in 2017.

V. APPENDIX

A. Invited and contributed talks

1. Divesh Aggarwal

   Invited talks at *PQC Asia forum* in November 2016 hosted by National Institute for Mathematical Sciences, IIM (Institute for Industrial Mathematics) at Seoul National University, Korea Cryptography Forum; *Workshop on lattice algorithms and cryptography*, in FSTTCS, December 2017.

2. Anurag Anshu

   Invited talks at *Information Theory Workshop*, 2017 (Kaoshiung, Taiwan) and *Quantum Innovators in Computer Science and Mathematics Workshop*, 2017 (IQC, Waterloo, Canada).

   Contributed talks at *Asian Quantum Information Science Conference*, 2017 (Singapore); *Beyond IID in Information Theory Workshop*, 2017 (Singapore); *Computational Complexity Conference (CCC)* 2017 (Riga, Latvia); *Quantum Information Processing (QIP)* 2017 (Seattle, USA); *Theory of Quantum Computation, Communication and Cryptography (TQC)* 2016, (Berlin, Germany), 27-29 September.

3. Dmitry Gavinsky

   Invited talk at *workshop CE-ITI/CMI/IUUK*, Prague, 2017.

4. Hartmut Klauck

   Contributed talk at *42nd International Symposium on Mathematical Foundations of Computer Science*, Aalborg, Denmark, August 2017

5. Iordanis Kerenidis

   Invited talks at *Quantum simulation, processing and communication*, Nice, June 2017; *Heilbronn: Quantum Algorithms Day*, Bristol, April 2017.

6. Anupam Prakash

   Contributed talks at *Innovations in Theoretical Computer Science*, Berkeley, 2017; *Quantum Information Processing*, Seattle, 2017.

7. Ansis Rosmanis

   Contributed talk at *17th Asian Quantum Information Science Conference*, Singapore, September 2017.

8. Miklos Santha

   Invited talk at *Mathematics in Movement, Day of the Mathematical Sciences Foundation of Paris*, Paris, May 2017.

   Contributed talk at *17th ACM Computational Complexity Conference*, Riga, Latvia, July 2017.

9. Jamie Sikora

   Tutorial talk at *QCRYPT 2017*, Santa Barbara, 2017.

   Contributed talks at *Canadian Mathematical Society (CMS) Winter Meeting* 2016, Niagara Falls, Canada, 2016; *Conference on Contextuality: Conceptual Issues, Operational Signatures, and Applications*, Waterloo, Canada, 2017; *SIAM Conference on Optimization* 2017, Vancouver, Canada, 2017.

10. Antonis Varviotis

    Contributed talks at *5th International Conference on Continuous Optimization*, Tokyo, August 2016; *SIAM Conference on Optimization*, Vancouver, May 2017.

11. Naqueeb Ahmad Warsi

    Invited talk at *Beyond IID in Information Theory*, Singapore, 2017.

    Contributed talk at *QCRYPT 2017*, Cambridge, UK, 2017.

B. Professional activities

1. Divesh Aggarwal served on the PC of TCC 2016, ICITS 2017. He co-organized a one day workshop on post-quantum cryptography in October 2016 in CQT.

2. Dmitry Gavinsky served on the PC of CCC'2017.

3. Rahul Jain served on the PC of FSTTCS 2017, TQC 2017, QIP 2018. He is an Associate Editor in the Journal of Computer and System Sciences (JCSS) since January 2016. He was a member of the Organizing Committee of AQIS 2017 at NUS.

4. Iordanis Kerenidis is in the editorial board of *International Journal of Quantum Information*.

5. Hartmut Klauck was the Chair of the Organizing Committee of AQIS 2017 at NUS.

6. Troy Lee served on the PC of AQIS 2017, TQC 2017, AQIS 2016. He was a member of the Organizing Committee of AQIS 2017 at NUS.

7. Miklos Santha is in the steering committee of FCT and in the editorial board of *International Journal of Quantum Information*. He was a member of the Organizing Committee of AQIS 2017 at NUS, and co-organized a one day workshop on post-quantum cryptography in October 2016 in CQT.

8. Antonios Varvitsiotis co-organized a mini-symposium on *Conic Optimization and Quantum Information Theory* at the 2017 SIAM Conference on Optimization.

9. Hoeteck Wee co-organized a one day workshop on post-quantum cryptography in October 2016 in CQT.

[1] D. Aggarwal and J. Briët. Revisiting the Sanders-Bogolyubov-Ruzsa theorem in $\mathbb{F}_p^n$ and its application to non-malleable codes. In *Proceedings of IEEE International Symposium on Information Theory*, pages 1322–1326, 2016.

[2] D. Aggarwal, K.-M. Chung, H.-H. Lin, and T. Vidick. A quantum-proof non-malleable extractor, with application to privacy amplification against active quantum adversaries. Technical report, arXiv:1710.00557, 2017.

[3] D. Aggarwal and C. Dubey. Improved hardness results for unique shortest vector problem. *Information Processing Letters*, 116(10):631–637, 2016.

[4] D. Aggarwal, K. Hosseini, and S. Lovett. Affine-malleable extractors, spectrum doubling, and application to privacy amplification. In *Proceedings of IEEE International Symposium on Information Theory*, pages 2913–2917, 2016.

[5] D. Aggarwal, A. Joux, A. Prakash, and M. Santha. A new public-key cryptosystem via Mersenne numbers. Technical report, Cryptology ePrint Archive, Report 2017/481.

[6] D. Aggarwal, T. Kazana, and M. Obremski. Inception makes non-malleable codes stronger. In *Proceedings of the 15th IACR Theory of Cryptography Conference*, 2017.

[7] D. Aggarwal and U. Maurer. Breaking RSA generically is equivalent to factoring. *IEEE Transactions on Information Theory*, 62(11):6251–6259, 2016.

[8] D. Aggarwal and P. Mukhopadhyay. Faster algorithms for SVP and CVP in the ℓ_∞ norm. Submitted, 2017.

[9] D. Aggarwal and O. Regev. A note on discrete gaussian combinations of lattice vectors. *Chicago Journal of Theoretical Computer Science*, 7:1–1, 2016.

[10] D. Aggarwal and N. Stephens-Davidowit. (gap/s)-eth hardness of svp. Unpublished Manuscript, 2017.

[11] A. Ambainis, K. Balodis, A. Belovs, T. Lee, M. Santha, and J. Smotrovs. Separations in query complexity based on pointer functions. *Journal of the ACM*, 64(5), Article No. 32 2017.

[12] A. Anshu, I. Arad, and A. Jain. How local is the information in tensor networks of matrix product states or projected entangled pairs states. *Phys. Rev. B*, 94(19):195143, 2016.

[13] A. Anshu, S. Ben-David, A. Garg, R. Jain, R. Kothari, and T. Lee. Separating quantum communication from approximate rank. In *Proceedings of the 32th IEEE Conference on Computational Complexity (CCC)*, 2017. In *Proceedings of the 21th Annual Conference on Quantum Information Processing*, 2018.

[14] A. Anshu, V. K. Devabathini, and R. Jain. Quantum communication using coherent rejection sampling. *Physical Review Letters*, 119(12):120506, 2017.

[15] A. Anshu, A. Garg, A. W. Harrow, and P. Yao. Lower bound on expected communication cost of quantum huffman coding. In *Proceedings of the 11th Conference on the Theory of Quantum Computation, Communication and Cryptography*, volume 61, pages 3:1–3:18, 2016.

[16] A. Anshu, D. Gavinsky, R. Jain, S. Kundu, T. Lee, P. Mukhopadhyay, M. Santha, and S. Sanyal. A composition theorem for randomized query complexity. In *Proceedings of the 37rd Foundations of Software Technology and Theoretical Computer Science*, 2017.

[17] A. Anshu, P. Høyer, M. Mhalla, and S. Perdrix. Contextuality in multipartite pseudo-telepathy graph games. In *Proceedings of the 21st International Symposium on Fundamentals of Computation Theory*, 2017.

[18] A. Anshu, M.-H. Hsieh, and R. Jain. Quantifying resources in general resource theory with catalysts. In *Proceedings of the 21th Annual Conference on Quantum Information Processing*, 2018.

[19] A. Anshu, R. Jain, P. Mukhopadhyay, A. Shayeghi, and P. Yao. New one shot quantum protocols with application to communication complexity. *IEEE Transactions on Information Theory*, 62(12):7566–7577, 2016.

[20] A. Anshu, R. Jain, and N. Warsi. Building blocks for communication over noisy quantum networks. In *Proceedings of the 21th Annual Conference on Quantum Information Processing*, 2018.

[21] A. Anshu, R. Jain, and N. Warsi. Quantum compression protocols over quantum networks. In *Proceedings of the 21th Annual Conference on Quantum Information Processing*, 2018.

[22] A. Anshu, R. Jain, and N. A. Warsi. A generalized quantum Slepian-Wolf. In *Proceedings of the 17th Asian Quantum Information Science Conference*, 2017.

[23] A. Anshu, R. Jain, and N. A. Warsi. A hypothesis testing approach for communication over entanglement assisted compound quantum channel. Technical report, arXiv:1706.08286, 2017.

[24] A. Anshu, R. Jain, and N. A. Warsi. Measurement compression with quantum side information using shared randomness. Technical report, arXiv:1703.02342, 2017.

[25] A. Anshu, R. Jain, and N. A. Warsi. A one-shot achievability result for quantum state redistribution. *IEEE Transactions on Information Theory*, 2017.

[26] A. Anshu, R. Jain, and N. A. Warsi. One shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach. Technical report, arXiv:1702.01940, 2017.
[27] A. Anshu, R. Jain, and N. A. Warsi. A unified approach to source and message compression. Technical report, arXiv:1707.03619, 2017.
[28] A. Anshu, D. Touchette, P. Yao, and N. Yu. Exponential separation of quantum communication and classical information. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 277–288, 2017.
[29] I. Arad and B. Katzir. A local set of constraints for the reduced density matrices of local hamiltonian eigenstates. Unpublished Manuscript, 2017.
[30] A. Atserias, L. Mančinska, D. Roberson, R. Šámal, S. Severini, and A. Varvitsiotis. Quantum and non-signalling graph isomorphisms. Technical report, arXiv:1611.09837, 2016.
[31] A. Belovs, G. Ivanyos, Y. Qiao, M. Santha, and S. Yang. On the polynomial parity argument complexity of the combinatorial nullstellensatz. In *Proceedings of the 32nd Computational Complexity Conference*, pages 30:1–30:24, 2017.
[32] A. Belovs and A. Rosmanis. Adversary lower bounds for the collision and the set equality problems. Technical report, arXiv: 1310.5185v4, 2017.
[33] V. Bhargava, G. Ivanyos, R. Mittal, and N. Saxena. Irreducibility and r-th root finding over finite fields. In *Proceedings of the ACM Conference on International Symposium on Symbolic and Algebraic Computation,*, pages 37–44, 2017.
[34] Z. Brakerski, R. Tsabary, V. Vaikuntanathan, and H. Wee. Private constrained PRFs (and more) from LWE. In *Proceedings of the Theory of Cryptography Conference*, 2017.
[35] A. Chailloux, G. Gutoski, and J. Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago Journal of Theoretical Computer Science*, (13), 2016.
[36] A. Chailloux and I. Kerenidis. Physical limitations of quantum cryptographic primitives - optimal bounds for quantum coin flipping and bit commitment. *SIAM Journal on Computing*, 2017.
[37] A. Chailloux, I. Kerenidis, and M. Lauriere. The information cost of quantum memoryless protocols. In *Proceedings of the 17th Asian Quantum Information Science Conference*, 2017.
[38] D. Gavinsky. Quantum versus classical simultaneity in communication complexity. Technical report, arXiv:1705.07211, 2017.
[39] D. Gavinsky, R. Jain, H. Klauck, S. Kundu, T. Lee, M. Santha, S. Sanyal, and J. Vihrovs. Quadratically tight relations for randomized query complexity. Technical report, arXiv: 1708.00822v1, 2017.
[40] D. Gavinsky, O. Meir, O. Weinstein, and A. Wigderson. Toward better formula lower bounds: the composition of a function and a universal relation. *SIAM Journal on Computing*, 46(1):114–131, 2017.
[41] D. Gavinsky and P. Pudlák. Partition expanders. *Theory of Computing Systems*, 60(3):378–395, 2017.
[42] A. Grilo, I. Kerenidis, and T. Zijlstra. Learning with errors is easy with quantum samples. Technical report, arXiv:1702.08255, 2017.
[43] G. Gutoski, A. Rosmanis, and J. Sikora. Fidelity of quantum strategies with applications to cryptography. In *Proceedings of the 12th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2017.
[44] G. Ivanyos, M. Karpinski, M. Santha, N. Saxena, and I. E. Shparlinski. Polynomial interpolation and identity testing from high powers over finite fields. *Algorithmica*, pages 1–16, 2017.
[45] 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. In *Proceedings of the SIAM: ACM-SIAM Symposium on Discrete Algorithms (to appear)*, 2018.
[46] G. Ivanyos, Y. Qiao, and K. Subrahmaniam. Non-commutative edmonds' problem and matrix semi-invariants. *Computational Complexity*, 26(3):717–763, 2017.
[47] G. Ivanyos and M. Santha. On solving systems of diagonal polynomial equations over finite fields. *Theoretical Computer Science*, 657:73–85, 2017.
[48] R. Jain, C.A. Miller, and Y. Shi. Parallel device-independent quantum key distribution. Technical report arXiv:1703.05426, 2017.
[49] S. Kannan, E. Mossel, S. Sanyal, and G. Yaroslavtsev. Linear sketching over $\mathbb{F}_2$. *Electronic Colloquium of Computational Complexity*, (TR16-174), 2017.
[50] I. Kerenidis and A. Prakash. Quantum gradient descent for linear systems and least squares. Technical report arXiv:1704.04992, 2017.
[51] I. Kerenidis and A. Prakash. Quantum recommendation systems. In *Proceedings of the Innovations in Theoretical Computer Science*, 2017.
[52] H. Klauck. The complexity of quantum disjointness. In *Proceedings of the 42nd International Symposium on Mathematical Foundations of Computer Science*, pages 15:1–15:13, 2017.
[53] N. Kumar, E. Diamanti, and I. Kerenidis. Efficient quantum communications with multiplexed co-

herent state fingerprints. *Phys. Rev. A*, 95:032337, 2017.
[54] T. Lee, Z. Wei, and R. Wolf. Some upper and lower bounds on positive semidefinite rank. *Mathematical Programming, Series A*, 162(1–2):495–521, 2017.
[55] L. Mančinska, D. Roberson, R. Šámal, S. Severini, and A. Varvitsiotis. Relaxations of graph isomorphisms. In *Proceedings of the Iternational Colloquium on Automata, Languages and Programming*, 2017.
[56] W. McCutcheon, A. Pappa, B. Bell, A. McMillan, A. Chailloux, M. M. T. Lawson, D. Markham, E. Diamanti, I. Kerenidis, J. Raritya, and M. Tame. Experimental verification of multipartite entanglement in quantum networks. *Nature Communications*, 7, 2016.
[57] A. Prakash, J. Sikora, A. Varvitsiotis, and Z. Wei. Completely positive semidefinite rank. *Mathematical Programming, Series A, First Online: 05 October 2017.*
[58] A. Prakash and A. Varvitsiotis. Matrix factorizations of correlation matrices and applications. Technical report, arXiv:1702.06305, 2017.
[59] J. Radhakrishnan, P. Sen, and N. A. Warsi. One-shot private classical capacity of quantum wiretap channel: Based on one-shot quantum covering lemma. Technical report, arXiv:1703.01932, 2017.
[60] S. Sanyal. One-way communication and non-adaptive decision tree. *Electronic Colloquium of Computational Complexity*, (TR17-152), 2017.
[61] E. Schoute, L. Mančinska, T. Islam, I. Kerenidis, and S. Wehner. Shortcuts to quantum network routing. Technical report, arXiv:1610.05238, 2017.
[62] J. Sikora. Simple, near-optimal quantum protocols for die-rolling. *Cryptography*, 1(2):11, 2017.
[63] J. Sikora and A. Varvitsiotis. Linear conic formulations for two-party correlations and values of nonlocal games. *Mathematical Programming, Series A*, 162(1):431–463, 2017.
[64] J. Sikora and Z. Wei. Device-independent characterizations of a shared quantum state independent of any bell inequalities. *Physical Review A*, 95:032103, 2017.
[65] J. Sikora and Z. Wei. Device-independent dimension tests in a multiparty Bell experiment. Technical report, arXiv:1707.03125, 2017.
[66] F. M. T. Lee and M. Santha. Improved quantum query algorithms for triangle finding and associativity testing. *Algorithmica*, 77(2):459–486, 2017.
[67] L. Wossnig, Z. Zhao, and A. Prakash. A quantum linear system algorithm for dense matrices. Technical report, arXiv:1704.06174, 2017.