Computer Science Project: Report 2017-2018

I. INTRODUCTION

This report covers the period of November 2017 until July 2018.

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.

To celebrate the 10th anniversary of CQT, we have organized a "Workshop on "Quantum Algorithms and Complexity Theory" (WQACT) 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 (until August 2018)
   Miklos Santha.

2. **Research Fellows**:
   Han-Hsuan Lin
   Anupam Prakash
   Ansis Rosmanis
   Swagato Sanyal
   Antonios Varvitsiotis
   Naqueeb Warsi.

3. **Ph.D students**: Anurag Anshu (graduated July 2018)
   Naresh Goud Buddu
   Srijita Kundu
   Debbie Lim
   Priyanka Mukhopadhyay (graduating August 2018)
   Erick Purwanto
   Maharshi Ray
   Siyi Yang.

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**: Alper Cakan (Bogazici University) 23 July-20 Sept.18
   Joao Miguel Lourenco (Imperial College London) 10 July-6 Oct. 18
   Lai Wenxing (Fudan University) 2 July-24 August 18
   Kyriakos Katsamaktis (University of Edinburgh) 4 June-2 August 18
   Kunal Mittal (IIT) 14 May-13 July 18
   Felix Klingelhoefer (ENS Lyon) 13 May-31 July 18
   Vijeth Tumkur Aradhya (IIT Hyderabad) 13 May-3 Augusut 18
   Wei Zi Chun (Univ. Waterloo) 5 May-31 August 18
   Rajendra Kumar (IIT Kanpur) 17 April-14 June 18
   Jevgenijs Vihrovs (University of Latvia) 5 Januar-4 April 18
   Arjun Goel, 14 Dec.-29 Dec. 17

3. **Temporary visitors**:
   Michel de Rougemont (Institut de Recherche en Informatique Fondamentale) 7 May-11 May 18
   Elisa Celis (Ecole Polytechnique Federale de Lausanne) 1 April-5 April 18
   Nisheeth Vishnoi (Ecole Polytechnique Federale de Lausanne) 1 April-5 April 18
   Jianwei Li (Chinese Academy of Sciences) 18 March-25 March 18
   Arthi Sundaram (University of Maryland) 19 Feb.-2 March 18
   Alexander Belov (University of Latvia) 17 Januar-3 March 18
   Maciej Obremski (Aarhus University) 10 Januar-23 Januar 18
   Tomasz Kazana (University of Warsaw) 10 Januar-23 Januar 18
   Zuo Huijuan (Hebei Normal University) 27 Nov.17-25 May 18
   Peter Wittek (ICFO) 26 Nov-23 Dec. 17
   Shweta Agrawal (IIT Madras) 19 Nov-23 Nov. 17.

III. RESEARCH HIGHLIGHTS

A. Algorithms and Complexity

1. In the paper "Quantum attacks on Bitcoin and how to protect against them" [1], we analyzed the two key features underlying the security of Bitcoin, proof-of-work and digital signatures, to vulnerability to attack by a large scale error corrected quantum computer. The proof-of-work in Bitcoin is a search problem, and with a quantum computer Grover's algorithm can be used to solve it using quadratically fewer hashes than are needed classically. However, specialized classical hardware called ASICs designed for mining Bitcoin are extremely fast, doing over 14 trillion hashes per second. We found that this speed advantage over relatively slow near-term quantum computers with clock speeds of around 66 MHz would cancel out the quadratic advantage given by Grover's algorithm, at the current difficulty level. On the other hand, the digital signature algorithm used by Bitcoin, which is based on the hardness of the Elliptic curve discrete logarithm problem, is completely insecure in the presence of an error corrected quantum computer with around 500,000 physical qubits. Fortunately, there are quantum secure digital signature algorithms available based on hashing or lattice problems that can be used instead, although these typically have signature sizes 20-50 times larger than those currently used in Bitcoin.

2. In [26] we proposed an algorithm for learning a linear function from a sample whose distribution depends only on the value taken by the function. The complexity of our procedure is simply exponential in the number of values taken by elements of the sample with positive probability, while polynomial in the other parameters of the input. We applied our result to obtain polynomial-time quantum algorithms for certain generalized shift problems. These problems include as a special case the hidden subgroup problem in a class of semidirect product groups.

3. In a recent paper [20], together with Eyal Bairey and Netanel Lindner we devised a new quantum algorithm to learn local Hamiltonians by sampling them in a steady state (e.g., an eigenstate of the system, a Gibbs state, etc). The algorithm exploits the non-commutativeness of the local Hamiltonian terms, which give rise to local constraints on the expectation values of local observables. The result is a simple and robust algorithm that can use the expectation values in a local patch of the system to deduce the local Hamiltonian terms in that patch. Therefore, for spatially local Hamiltonians, the algorithm enables one to recover the underlying Hamiltonian in *linear time*. In the paper we also showed how the algorithm can be adapted to learn the Hamiltonian from dynamics.

B. Communication Complexity, Query Complexity and Other Aspects of Communication

1. A central question in classical information theory is that of source compression, which is the task where Alice receives a sample from a known probability distribution and needs to transmit it to the receiver Bob with small error. This problem has a one-shot solution due to Huffman, in which the messages are of variable length and the expected length of the messages matches the asymptotic and i.i.d. compression rate of the Shannon entropy of the source. In [9], we consider a quantum extension of above task, where Alice receives a sample from a known probability distribution and needs to transmit a part of a pure quantum state (that is associated to the sample) to Bob. We allow entanglement assistance in the protocol, so that the communication is possible through classical messages, for example using quantum teleportation. The classical messages can have a variable length and the goal is to minimize their expected length. We provide a characterization of the expected communication cost of this task, by giving a lower bound that is near optimal up to some additive factors. A special case of above task, and the quantum analogue of the source compression problem, is when Alice needs to transmit a pure quantum state. Here we show that there is no one-shot interactive scheme which matches the asymptotic and i.i.d. compression rate of the von

Neumann entropy of the average quantum state. This is a relatively rare case in quantum information theory where the cost of a quantum task is significantly different from its classical analogue. Further, we also exhibit similar results for the fully quantum task of quantum state redistribution, employing some different techniques. We show implications for the one-shot version of the problem of quantum channel simulation.

2. In [12] we consider a general resource theory that allows the use of free resource as a catalyst. We show that the amount of 'resource' contained in a given state, in the asymptotic scenario, is equal to the regularized relative entropy of resource of that state, which then yields a straightforward operational meaning to this quantity. Such an answer has been long sought for in any resource theory since the usefulness of a state in information-processing tasks is directly related to the amount of resource the state possesses in the beginning. While we need to place a few assumptions in our resource theoretical framework, it is still general enough and includes quantum resource theory of entanglement, coherence, asymmetry, non-uniformity, purity, contextuality, stabilizer computation and the classical resource theory of randomness extraction as special cases. Since our resource theoretic framework includes entanglement theory, our result also implies that the amount of noise one has to inject locally in order to erase all entanglement contained in an entangled state is equal to the regularized relative entropy of entanglement, resolving an open question posted in [Groisman et al., Phys. Rev. A. 72: 032317, 2005]. On the way to prove the main result, we also quantify the amount of resource contained in a state in the one-shot setting (where one only has a single copy of the state), in terms of the smooth max-relative entropy. Our one-shot result employs a recently developed technique of convex-split lemma.

3. The capacity of a quantum channel characterizes the limits of reliable communication through a noisy quantum channel. This fundamental information theoretic question is very well studied specially in the setting of many independent uses of the channel. An important scenario, both from practical and conceptual point of view, is when the channel can be used only once. This is known as the one-shot channel coding problem. In [14] we provide a tight characterization of the one-shot entanglement assisted classical capacity of a quantum channel. We arrive at our result by introducing a simple decoding technique which we refer to as position-based decoding. We also consider two other important quantum network scenarios: quantum channel with a jammer and quantum broadcast channel. For these problems, we use the recently introduced convex split technique in addition to position based decoding. Our approach exhibits that the simultaneous use of these two techniques provides a uniform and conceptually simple framework for designing communication protocols for quantum networks.

4. In [15], we study the problem of entanglement-assisted quantum state redistribution in the one-shot setting and provide a new achievability result on the quantum communication required. Our bounds are in terms of the max-relative entropy and the hypothesis testing relative entropy. We use the techniques of convex split and position-based decoding to arrive at our result. We show that our result is upper bounded by the result obtained in Berta et al. (2016).

5. In [17], we consider a quantum generalization of the task considered by Slepian and Wolf regarding distributed source compression. In our task, Alice, Bob, Charlie, and Reference share a joint pure state. Alice and Bob wish to send a part of their respective systems to Charlie without collaborating with each other. We give achievability bounds for this task in the one-shot setting and provide the asymptotic and independent identically distributed analysis in the case when there is no side information with Charlie. Our result implies the result of Abeyesinghe et al., who studied a special case of this problem. As another special case wherein Bob holds trivial registers, we recover the result of Devetak and Yard regarding quantum state redistribution.

6. In [11] we study the problem of secure communication over a fully quantum Gel'fand-Pinsker channel. One key feature of the results obtained in this work is that all the bounds obtained

are in terms of error exponent. We obtain our achievability result via the technique of simultaneous pinching. This in turn allows us to show the existence of a simultaneous decoder. Further, to obtain our encoding technique and to prove the security feature of our coding scheme we prove a bivariate classical-quantum channel resolvability lemma and a conditional classical-quantum channel resolvability lemma. As a by product of the achievability result obtained in this work, we also obtain an achievable rate for a fully quantum Gel'fand-Pinsker channel in the absence of Eve. The form of this achievable rate matches with its classical counterpart. The Gel'fand-Pinsker channel model had earlier only been studied for the classical-quantum case and in the case where Alice (the sender) and Bob (the receiver) have shared entanglement between them.

7. In [13] we study the problem of communication over compound quantum channel in the presence of entanglement. Classically such channels are modeled as a collection of conditional probability distributions wherein neither the sender nor the receiver is aware of the channel being used for transmission, except for the fact that it belongs to this collection. We provide achievability and converse bounds for this problem in the one shot quantum setting in terms of quantum hypothesis testing divergence. We also consider the case of informed sender, showing a one shot achievability result that converges appropriately in the asymptotic i.i.d. setting. Our achievability proof is similar in spirit to its classical counterpart. To arrive at our result, we use the technique of *position based decoding* along with a new approach for constructing a *union* of two projectors, which can be of independent interest.

8. In [16] we study the problem of transmission of classical messages through a quantum channel in several network scenarios in the one-shot setting. We consider both the entanglement assisted and unassisted cases for the point to point quantum channel, quantum multiple-access channel, quantum channel with state and the quantum broadcast channel. We show that it is possible to near-optimally characterize the amount of communication that can be transmitted in these scenarios, using the position-based decoding strategy introduced in [14]. In the process, we provide a short and elementary proof of the converse for entanglement-assisted quantum channel coding in terms of the quantum hypothesis testing divergence (obtained earlier by Mathews and Wehner). Our proof has the additional utility that it naturally extends to various network scenarios mentioned above. Furthermore, none of our achievability results require a *simultaneous decoding* strategy, existence of which is an important open question in quantum Shannon theory.

9. It is well known that transmitting classical information over quantum networks can significantly improve communication rates and achieve secure communication. These quantum advantages crucially rely on the networks innate ability to distribute classical correlations reliably and securely. To this end, it is of significant interest to understand how classical information propagates in quantum networks. In [32] we report a computational toolbox that is able to characterise the stochastic matrix of any classical-quantum network, assuming only the inner-product information of the quantum code states. The toolbox is hence highly versatile and can analyse a wide range of quantum network protocols, including those that employ infinite-dimensional quantum states. To demonstrate the feasibility and efficacy of our toolbox, we use it to reveal new results in multipartite quantum distributed computing and quantum cryptography. Taken together, these findings suggest that our method may have important implications for quantum network information theory and the development of new quantum technologies.

10. In [30] we study quantum communication protocols, in which the players' storage starts out in a state where one qubit is in a pure state, and all other qubits are totally mixed (i.e. in a random state), and no other storage is available (for messages or internal computations). This restriction on the available quantum memory has been studied extensively in the model of quantum circuits, and it is known that classically simulating quantum circuits operating on such memory is hard when the additive error of the simulation is exponentially small (in the input length), under the assumption that the polynomial hierarchy does not collapse.

We study this setting in communication complexity. The goal is to consider larger additive error for simulation-hardness results, and to not use unproven assumptions.

We define a complexity measure for this model that takes into account that standard error reduction techniques do not work here. We define a clocked and a semi-unclocked model, and describe efficient simulations between those.

We characterize a one-way communication version of the model in terms of weakly unbounded error communication complexity.

Our main result is that there is a quantum protocol using one clean qubit only and using $O(\log n)$ qubits of communication, such that any classical protocol simulating the acceptance behaviour of the quantum protocol within additive error $1/poly(n)$ needs communication $\Omega(n)$.

We also describe a candidate problem, for which an exponential gap between the one-clean-qubit communication complexity and the randomized complexity is likely to hold, and hence a classical simulation of the one-clean-qubit model within *constant* additive error might be hard in communication complexity. We describe a geometrical conjecture that implies the lower bound.

11. Wiesners unforgeable quantum money scheme is widely celebrated as the first quantum information application. Nevertheless, despite its central role in quantum cryptography, its experimental implementation has remained elusive because of the lack of realistic protocols adapted to practical quantum storage devices and verification techniques. In [21] we experimentally demonstrate a quantum money protocol that rigorously satisfies the security condition for unforgeability, using a practical system exploiting single-photon polarization encoding of highly attenuated coherent states of light for on-the-fly credit card state generation and readout. Our implementation includes classical verification and is designed to be compatible with state-of-the-art quantum memories, which have been taken into account in the security analysis, together with all system imperfections. Our results constitute a major step towards a real-world realization of this milestone quantum information protocol.

C. Quantum safe cryptography

1. Hardness of SVP under the exponential time hypothesis.

   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 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 $p > 2$, there is no $2^{o(n)}$-time algorithm for SVP in the ℓ_p norm unless (randomized) Gap Exponential time Hypothesis (Gap-ETH) fails.

- There is no $2^{o(n)}$-time algorithm for SVP in the ℓ_2 norm unless either (1) (non-uniform) Gap-ETH is false; or (2) the lattice kissing number is $2^{o(n)}$.

2. In [3] we propose a new public-key cryptosystem whose security is based on the computational intractability of the following problem: Given a Mersenne number $p = 2^n - 1$, where n is a prime, a positive integer h, and two n-but integers T, R, find two n-bit integers F, G each of Hamming weight at most h such that $T = F \cdot R + G$ modulo p, under the promise that they exist.

   This work was also submitted on 30 November 2017 to the call for proposals of the National Institute of Standard (NIST) to evaluate and standardize one or more quantum-resistant cryptographic algorithms. It is listed among the 1st round submissions at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions. It was also presented at the First PQC Standardization Conference in Fort Lauderdale, Florida, in April 2018.

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.

IV. TEACHING AND OUTREACH

A. Teaching

1. Divesh Aggarwal course on *Computational Complexity* (C5230), NUS, Spring 2018.
2. Rahul Jain course on *Introduction to Information Theory* (CS3236), NUS, Spring 2018.
3. Hartmut Klauck course on *Computational Economics* (MH4320), NTU, Fall 2017; course on *Discrete Mathematics* (MH 1301), NTU, Spring 2018.
4. Troy Lee course on *Linear Algebra I* (MH1200) NTU, Fall 2017.
5. Antonios Varvitsiotis course on *Convex Optimization and Quantum Foundations* (QT5201N), NUS, Spring 2017.

B. Outreach

1. Troy Lee: Pint of Science talk at Esplanade May 15, 2018; Talk at Accenture workshop April 5, 2018; Public lecture at Innovfest June 5, 2018.
2. Srijita Kundu: Co-organizer and lecturer for QCamp-18.

V. ALUMNI UPDATES

1. Penghui Yao (in our group 2009-14), has joined Nanjing University (https://www.nju.edu.cn/EN/), China as Assistant Professor. He has also obtained a fellowship under the coveted "Thousand Talents" program (http://www.1000plan.org/en/) of the Chinese government.
2. Swagato Sanyal (in our group 2017-18) has joined Department of Computer Science, Indian Institute of Technology, Kharagpur (IIT KGP) as Assistant Professor.

VI. APPENDIX

A. Invited and contributed talks

1. Divesh Aggarwal

   Invited talk in a workshop on lattice algorithms and cryptography in FSTTCS, December 2017. Invited talk in IISC-IACR School on Cryptology, January, 2018.

2. Anurag Anshu

   Invited talks:
   "Noisy quantum state redistribution and the Alpha-bit," at Rocky Mountain Summit on Quantum Information, University of Colorado Boulder, June 25-29, 2018.
   "Achievability bounds on quantum state redistribution using convex split and position based decoding," at Information Theory Workshop, Kaohsiung, Taiwan, November 6-10 2017.
   "Protocols for communication over quantum networks," at Quantum Innovators Workshop, Waterloo, Canada, September 18-22, 2017.

   Contributed talks:
   "A hypothesis testing approach for communication over compound quantum channel," at IEEE International Symposium on Information Theory (ISIT), Colorado, USA, June 17-22, 2018.
   "Building blocks for communication over noisy quantum networks," at ISIT, Colorado, USA, June 17-22, 2018.
   "Expected communication cost of distributed quantum tasks," at ISIT, Colorado, USA, June 17-22, 2018.
   "The cost of destroying entanglement and resource," at 21st QIP, Delft, Jan.13-19, 2018.
   "Protocols for communication over quantum networks," at 21st QIP, Delft, Jan.13-19, 2018.

3. Dmitry Gavinsky

   Invited talk at WQACT'18.

4. Gabor Ivanyos

   Invited talk at the workshop on Optimization, Complexity and Invariant Theory (OCIT 2018).

5. Rahul Jain

   Invited talks at:
   "Quantum Communication Using Coherent Rejection Sampling," at International Conference on Signal Processing and Communications (SPCOM), Indian Institute of Science (IISC), Bangalore, India, 2018.
   Bombay Information Theory Seminar (BITS), Mumbai, India. January 2018.
   Conference on "Quantum Information Theory". The Henri Poincaré Institute. Paris, France. December 2017.

6. Iordanis Kerenidis

   Talks at Challenges in Quantum Computation Summer Cluster (Berkeley, June 2018); Workshop on Quantum Algorithms and Complexity Theory, Centre for Quantum Technologies (Singapore, March 2018); Forum du CNRS (Paris, November 2017).

7. Troy Lee

   Invited to panel discussion at the cyber security conference Cycon, June 1 2018; Speaker at Quantum-safe Communications Workshop July 17, 2018.

8. Anupam Prakash

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

9. Naqueeb Warsi:

   Contributed talk:
   "One-shot private classical capacity of quantum wiretap channel: Based on one-shot quantum covering lemma," at 7th QCrypt, University of Cambridge, September 18-22, 2017.

10. Miklos Santha

    Invited talks at *Fraunhofer Workshop on Post-Quantum Cryptography in Practice*, Singapore, February 2018 *Workshop on Algebraic Complexity Theory*, Paris, May 2018 *French Academy of Sciences*, Paris, May 2018

B. Awards

1. Anurag Anshu won "Dean's Graduate Research Excellence Award, 2018" awarded for distinguished thesis at School of Computing, NUS. (https://www.quantumlah.org/about/highlight.php?id=293)

2. Rahul Jain received award under the "VAJRA (Visiting Advanced Joint Research) Faculty Scheme" (http://vajra-india.in/) of the Science and Engineering Board (SERB) of the Department of Science and Technology (DST), Government of India.

3. Following paper listed among "Best of 2016" by ACM Computing Reviews:
   Lila Fontes, Rahul Jain, Iordanis Kerenidis, Mathieu Laurière, Sophie Laplante and Jérémie Roland. "Relative discrepancy does not separate information and communication complexity." In proceedings of The 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015), vol. 9134, LNCS, pp. 506-516, 2015.

C. Professional activities

1. Divesh Aggarwal served on the PC of TCC 2018, SPACE 2018.

2. Rahul Jain served on the PC of QIP 2018 and TQC 2018. He is an Associate Editor in the Journal of Computer and System Sciences (JCSS) since January 2016.

3. Gabor Ivanyos served on the PC of the 2018 International Symposium on Symbolic and Algebraic Computation (ISSAC 2018).

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

5. Troy Lee was on the Program Committee of ICALP 2018.

6. Miklos Santha is in the steering committee of FCT and in the editorial board of *International Journal of Quantum Information.*

[1] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel. Quantum attacks on Bitcoin and how to protect against them. *Ledger*, 2018.

[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, A. Joux, A. Prakash, and M. Santha. A new public-key cryptosystem via mersenne numbers. In *38th International Cryptology Conference CRYPTO*, 2018.

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

[5] D. Aggarwal, T. Kazana, and M. Obremski. Leakage-resilient algebraic manipulation detection codes with optimal parameters. Cryptology ePrint Archive, Report 2018/058, 2018.

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

[7] D. Aggarwal and N. Stephens-Davidowitz. (gap/s) eth hardness of svp. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 228–238. ACM, 2018.

[8] D. Aggarwal and N. Stephens-Davidowitz. Just take the average! an embarrassingly simple 2^n-time algorithm for svp (and cvp). In *Proceedings of the Symposium on Simplicity in Algorithms (to appear)*, 2018.

[9] A. Anshu, A. Garg, A. W. Harrow, and P. Yao. Expected communication cost of distributed quantum tasks. *IEEE Transactions on Information Theory*, pages 1–1, 2018.

[10] 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 *37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 10:1–10:13, 2017.

[11] A. Anshu, M. Hayashi, and N. A. Warsi. Secure communication over fully quantum gel'fand-pinsker wiretap channel. arXiv:1801.00940, 2018.

[12] A. Anshu, M.-H. Hsieh, and R. Jain. Quantifying resource in catalytic resource theory. To appear in Physical Review Letters, 2018.

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

[14] A. Anshu, R. Jain, and N. A. Warsi. Building blocks for communication over noisy quantum networks. *IEEE Transactions on Information Theory*, pages 1–1, 2018.

[15] A. Anshu, R. Jain, and N. A. Warsi. A generalized quantum slepian-wolf. *IEEE Transactions on Information Theory*, 64(3):1436–1453, March 2018.

[16] A. Anshu, R. Jain, and N. A. Warsi. On the near-optimality of one-shot classical communication over quantum channels. arXiv:1804.09644, 2018.

[17] A. Anshu, R. Jain, and N. A. Warsi. A one-shot achievability result for quantum state redistribution. *IEEE Transactions on Information Theory*, 64(3):1425–1435, March 2018.

[18] I. Arad, M. Santha, A. Sundaram, and S. Zhang. Linear time algorithm for quantum 2sat. *Theory of Computing*, pages 1–27, 2018.

[19] J. Arrazola, E. Diamanti, and I. Kerenidis. Quantum superiority for verifying np-complete problems with linear optics. Technical Report quant-ph/1711.02200, arXiv, 2017.

[20] E. Bairey, I. Arad, and N. H. Lindner. Learning a local hamiltonian from local measurements. *arXiv preprint arXiv:1807.04564*, 2018.

[21] M. Bozzio, A. Orieux, L. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti. Experimental investigation of practical unforgeable quantum money. *npj Quantum Information*, 4, 2018.

[22] A. Chailloux and I. Kerenidis. Physical limitations of quantum cryptographic primitives or optimal bounds for quantum coin flipping and bit commitment. *SIAM Journal on Computing*, 46:1647–1677, 2017.

[23] C. Godsil, D. E. Roberson, B. Rooney, R. Šamal, and A. Varvitsiotis. Vector coloring the categorical product of graphs. Technical Report arXiv:1801.08243, arXiv, 2018.

[24] G. Ivanyos, M. Karpinski, M. Santha, N. Saxena, and I. E. Shparlinski. Polynomial interpolation and identity testing from high powers over finite fields. *Algorithmica*, 80:560–575, 2018. Acceptance reported last year.

[25] G. Ivanyos, R. Kulkarni, Y. Qiao, M. Santha, and A. Sundaram. On the complexity of trial and error for constraint satisfaction problems. *J. Comput. Syst. Sci.*, 92:48–64, 2018. Journal version of an earlier conference paper.

[26] G. Ivanyos, A. Prakash, and M. Santha. On learning linear functions from subset and its applications in quantum computing. In *Proceedings of the Twenty-Sixth European Symposium on Algorithms,*

ESA'18, (LIPIcs Vol. 112), pages 66:1–12. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018. Preprint: arXiv:1806.09660 (quant-ph).

[27] 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 Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pages 2357–2376, 2018. Acceptance reported last year.

[28] R. Jain, H. Klauck, S. Kundu, T. Lee, M. Santha, S. Sanyal, and J. Vihrovs. Quadratically tight relations for randomized query complexity. In *13th International Computer Science Symposium in Russia, CSR*, pages 207–219, 2018.

[29] I. Kerenidis and A. Luongo. Quantum classification of the mnist dataset via slow feature analysis. Technical Report quant-ph/1805.08837, arXiv, 2018.

[30] H. Klauck and D. Lim. The power of one clean qubit in communication complexity. Technical report, arxiv:1807.07762.

[31] N. Kumar, E. Diamanti, and I. Kerenidis. Efficient quantum communications with coherent state fingerprints over multiple channels. *Physical Review A*, 95, 2017.

[32] Y. Wang, W. Primaatmaja, A. Varvitsiotis, and C. C. W. Lim. Characterising the behaviour of classical-quantum broadcast networks. In *Proceedings of the 8th International Conference on Quantum Cryptography*, 2018.

[33] L. Wossnig, Z. Zhao, and A. Prakash. A quantum linear system algorithm for dense matrices. *Physical Review Letters*, 120, 2018.