REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
29-05-2016	Final Report	1-Sep-2012 - 29-Feb-2016

4. TITLE AND SUBTITLE

Final Report: Research on Quantum Algorithms at the Institute for Quantum Information and Matter

5a. CONTRACT NUMBER
W911NF-12-1-0521

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS

John Preskill

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

California Institute of Technology
Office of Sponsored Research
1200 E. California Blvd.
Pasadena, CA 91125 -0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
62379-PH-OC.113

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

The central goals of our project are (1) to bring large-scale quantum computers closer to realization by proposing and analyzing new schemes for protecting quantum systems from noise, and (2) to conceive, develop, and analyze new applications of quantum computing to physics and mathematics.

15. SUBJECT TERMS

quantum algorithms, quantum complexity, fault-tolerant quantum computing

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John Preskill
UU	UU	UU	UU		19b. TELEPHONE NUMBER 626-395-6691

Report Title

Final Report: Research on Quantum Algorithms at the Institute for Quantum Information and Matter

ABSTRACT

The central goals of our project are (1) to bring large-scale quantum computers closer to realization by proposing and analyzing new schemes for protecting quantum systems from noise, and (2) to conceive, develop, and analyze new applications of quantum computing to physics and mathematics.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper
05/26/2016 78.00	John_Napp, John_Preskill. Optimal Bacon-Shor codes, Quantum Information and Computation, (05 2013): 490. doi:
05/29/2016 80.00	Matthew_Hastings , Spyridon_Michalakis. Quantization of Hall Conductance For Interacting Electrons on a Torus, Commun. Math. Phys., (09 2014): 433. doi:
05/29/2016 79.00	I. H. Kim. Long-range entanglement is necessary for a topological storage of quantum information, Phys. Rev. Lett. (accepted), (08 2013): 80503. doi:
05/29/2016 04.00	Fernando_Pastawski , John_Preskill. Error correction for encoded quantum annealing, PHYSICAL REVIEW A , (05 2016): 52325. doi:
05/29/2016 03.00	Gilad_Goura , Markus_P._Müllerc , Varun_Narasimhachara , Robert_W._Spekkens , Nicole_Yunger_Halpern. The resource theory of informational nonequilibrium inthermodynamics, Physics Reports, (07 2015): 1. doi:
05/29/2016 02.00	Nicole_Yunger_Halpern, Joseph_M._Renes. Beyond heat baths: Generalized resource theories for small-scale thermodynamics, Physical Review E, (02 2016): 22126. doi:
05/29/2016 01.00	Toby_Cubitt, Michael_Kastoryano, Ashley_Montanaro, Kristan_Temme. Quantum reverse hypercontractivity, Journal of Mathematical Physics, (10 2015): 102204. doi:
05/29/2016 00.00	Michael_Beverland, Oliver_Buerschaper, Robert_Koenig, Fernando_Pastawski, John_Preskill, Sumit_Sijher. Protected gates for topological quantum field theories, Journal of Mathematical Physics, (01 2016): 22201. doi:
05/29/2016 99.00	Fernando_Pastawski, Beni_Yoshida. Fault-tolerant logical gates in quantum error-correcting codes, PHYSICAL REVIEW A , (01 2015): 12305. doi:
05/29/2016 98.00	Angelo_Lucia, Toby_S._Cubitt, Spyridon_Michalakis, David_Perez-Garcia. Rapid mixing and stability of quantum dissipative systems, PHYSICAL REVIEW A , (04 2015): 40302. doi:
05/29/2016 97.00	Olivier_Landon-Cardinal, Beni_Yoshida, David_Poulin, John_Preskill. Perturbative instability of quantum memory based on effective long-range interactions, PHYSICAL REVIEW A , (03 2015): 32303. doi:
05/29/2016 94.00	David_Sutter, Omar_Fawzi, Renato_Renner. Universal recovery map forapproximate Markov chains, Royal Society, (01 2016): 20150623. doi:
05/29/2016 93.00	Mario_Berta, Matthias_Christandl, Dave_Touchette. Smooth Entropy Bounds on One-ShotQuantum State Redistribution, IEEE TRANSACTIONS ON INFORMATION THEORY, (03 2016): 1425. doi:
05/29/2016 92.00	Mario_Berta, Marius_Lemmy, Mark_M._Wilde. Monotonicity of quantum relative entropy and recoverability, Quantum Information & Computation, (11 2015): 1333. doi:

05/29/2016 91.00 Mario_Berta, Marco_Tomamichel. The Fidelity of Recovery Is Multiplicative,
IEEE Transaction on Information Theory, (04 2016): 1758. doi:

05/29/2016 90.00 Marco_Tomamichel, Mario_Berta, Joseph_M._Renes. Quantum coding with finite resources,
Nature Communications, (05 2016): 11419. doi:

05/29/2016 88.00 Mario_Berta, Joseph_M._Renes, Mark_M._Wilde. Identifying the Information Gain of a Quantum Measurement ,
IEEE TRANSACTIONS ON INFORMATION THEORY, (10 2014): 331. doi:

05/29/2016 87.00 Mario_Berta, Patrick_Coles, Stephanie_Wehner. Entanglement-assisted guessing of complementary measurement outcomes,
PHYSICAL REVIEW A , (12 2014): 62127. doi:

05/29/2016 86.00 Ning_Bao, Sepehr_Nezami, Hirosi_Ooguri, Bogdan_Stoica, James_Sullye, Michael_Walter. The holographic entropy cone,
Journal of High Energy Physics, (09 2015): 130. doi:

05/29/2016 85.00 Ning_Bao, ChunJun_Cao, Sean_M_Carroll, Aidan_Chatwin-Davies, Nicholas_Hunter-Jones, Jason_Pollack, Grant_N._Remmen. Consistency conditions for an AdS multiscale entanglement renormalization ansatz correspondence ,
PHYSICAL REVIEW D, (06 2015): 125036. doi:

05/29/2016 84.00 Kristan_Temme, Fernando_Pastawski, Michael_Kastoryano. Hypercontractivity of quasi-free quantumsemigroups,
Journal of Physics A: Mathematical and Theoretical, (09 2014): 405303. doi:

05/29/2016 83.00 G_Vidal, Glen_Evenbly. Real-Space Decoupling Transformation for Quantum Many-Body Systems,
Physical Review Letters (accepted), (06 2014): 220502. doi:

05/29/2016 82.00 John_Preskill. SUFFICIENT CONDITION ON NOISE CORRELATIONSFOR SCALABLE QUANTUM COMPUTING,
Quant. Inf. Comput, (03 2013): 181. doi:

10/22/2015 16.00 J. Ignacio Cirac, Didier Poilblanc, Norbert Schuch, Frank Verstraete. Entanglement spectrum and boundary theories with projected entangled-pair states,
Physical Review B, (06 2011): 0. doi: 10.1103/PhysRevB.83.245134

10/22/2015 37.00 J. Ignacio Cirac, Spyridon Michalakis, David Pérez-García, Norbert Schuch. Robustness in projected entangled pair states,
Physical Review B, (09 2013): 0. doi: 10.1103/PhysRevB.88.115108

10/22/2015 36.00 Toby S. Cubitt, Angelo Lucia, Spyridon Michalakis, David Perez-Garcia. Stability of Local Quantum Dissipative Systems,
Communications in Mathematical Physics, (04 2015): 0. doi: 10.1007/s00220-015-2355-3

10/22/2015 35.00 Peter Brooks, John Preskill. Fault-tolerant quantum computation with asymmetric Bacon-Shor codes,
Physical Review A, (03 2013): 0. doi: 10.1103/PhysRevA.87.032310

10/22/2015 34.00 Jutho Haegeman, Spyridon Michalakis, Bruno Nachtergaele, Tobias J. Osborne, Norbert Schuch, Frank Verstraete. Elementary Excitations in Gapped Quantum Spin Systems,
Physical Review Letters, (08 2013): 0. doi: 10.1103/PhysRevLett.111.080401

10/22/2015 33.00 Matthew B. Hastings, Spyridon Michalakis. Quantization of Hall Conductance for Interacting Electrons on a Torus,
Communications in Mathematical Physics, (09 2014): 0. doi: 10.1007/s00220-014-2167-x

10/22/2015 32.00 Isaac H. Kim. Perturbative analysis of topological entanglement entropy from conditional independence,
Physical Review B, (12 2012): 0. doi: 10.1103/PhysRevB.86.245116

10/22/2015 31.00 Isaac H. Kim. Determining the structure of the real-space entanglement spectrum from approximate conditional independence,
Physical Review B, (04 2013): 0. doi: 10.1103/PhysRevB.87.155120

10/22/2015 30.00 Isaac H. Kim. Operator extension of strong subadditivity of entropy,
Journal of Mathematical Physics, (2012): 0. doi: 10.1063/1.4769176

10/22/2015 29.00 Isaac H. Kim. Long-Range Entanglement Is Necessary for a Topological Storage of Quantum Information,
Physical Review Letters, (08 2013): 0. doi: 10.1103/PhysRevLett.111.080503

10/22/2015 28.00 Sergey Bravyi, Jeongwan Haah. Magic-state distillation with low overhead,
Physical Review A, (11 2012): 0. doi: 10.1103/PhysRevA.86.052329

10/22/2015 26.00 G. Evenbly, G. Vidal. Class of Highly Entangled Many-Body States that can be Efficiently Simulated,
Physical Review Letters, (06 2014): 0. doi: 10.1103/PhysRevLett.112.240502

10/22/2015 15.00 Lukasz Fidkowski, Alexei Kitaev. Topological phases of fermions in one dimension,
Physical Review B, (02 2011): 0. doi: 10.1103/PhysRevB.83.075103

10/22/2015 12.00 Liang Jiang, Takuya Kitagawa, Jason Alicea, A. R. Akhmerov, David Pekker, Gil Refael, J. Ignacio Cirac, Eugene Demler, Mikhail D. Lukin, Peter Zoller. Majorana Fermions in Equilibrium and in Driven Cold-Atom Quantum Wires,
Physical Review Letters, (06 2011): 0. doi: 10.1103/PhysRevLett.106.220402

10/22/2015 13.00 Courtney G Brell, Steven T Flammia, Stephen D Bartlett, Andrew C Doherty. Toric codes and quantum doubles from two-body Hamiltonians,
New Journal of Physics, (05 2011): 0. doi: 10.1088/1367-2630/13/5/053039

10/22/2015 14.00 N. Y. Yao, L. Jiang, A. V. Gorshkov, Z.-X. Gong, A. Zhai, L.-M. Duan, M. D. Lukin. Robust Quantum State Transfer in Random Unpolarized Spin Chains,
Physical Review Letters, (01 2011): 0. doi: 10.1103/PhysRevLett.106.040505

10/22/2015 1.00 Ersen Bilgin, Sergio Boixo. Preparing Thermal States of Quantum Systems by Dimension Reduction,
Physical Review Letters, (10 2010): 0. doi: 10.1103/PhysRevLett.105.170405

10/22/2015 2.00 Steven T. Flammia, Yi-Kai Liu. Direct Fidelity Estimation from Few Pauli Measurements,
Physical Review Letters, (06 2011): 0. doi: 10.1103/PhysRevLett.106.230501

10/22/2015 3.00 Salman Beigi, Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography,
New Journal of Physics, (09 2011): 0. doi: 10.1088/1367-2630/13/9/093036

10/22/2015 4.00 Marcus Cramer, Martin B. Plenio, Steven T. Flammia, Rolando Somma, David Gross, Stephen D. Bartlett, Olivier Landon-Cardinal, David Poulin, Yi-Kai Liu. Efficient quantum state tomography,
Nature Communications, (12 2010): 0. doi: 10.1038/ncomms1147

10/22/2015 5.00 Prabha Mandayam, Stephanie Wehner. Achieving the physical limits of the bounded-storage model,
Physical Review A, (02 2011): 0. doi: 10.1103/PhysRevA.83.022329

10/22/2015 6.00 D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, A. Winter. Operational interpretations of quantum discord,
Physical Review A, (03 2011): 0. doi: 10.1103/PhysRevA.83.032324

10/22/2015 7.00 Jeongwan Haah. Local stabilizer codes in three dimensions without string logical operators,
Physical Review A, (04 2011): 0. doi: 10.1103/PhysRevA.83.042330

10/22/2015 8.00 Sergey Bravyi, Jeongwan Haah. Energy Landscape of 3D Spin Hamiltonians with Topological Order,
Physical Review Letters, (10 2011): 0. doi: 10.1103/PhysRevLett.107.150504

10/22/2015 9.00 Jeongwan Haah, John Preskill. Logical-operator tradeoff for local quantum codes,
Physical Review A, (09 2012): 0. doi: 10.1103/PhysRevA.86.032308

10/22/2015 10.00 Liang Jiang, Charles L. Kane, John Preskill. Interface between Topological and Superconducting Qubits, Physical Review Letters, (03 2011): 0. doi: 10.1103/PhysRevLett.106.130504

10/22/2015 11.00 Liang Jiang, Adilet Imambekov. Universal dynamical decoupling of multiqubit states from environment, Physical Review A, (12 2011): 0. doi: 10.1103/PhysRevA.84.060302

10/23/2015 69.00 Aleksander Kubica, Beni Yoshida, Fernando Pastawski. Unfolding the color code, New Journal of Physics, (08 2015): 0. doi: 10.1088/1367-2630/17/8/083026

10/23/2015 70.00 Fernando Pastawski, Beni Yoshida. Fault-tolerant logical gates in quantum error-correcting codes, Physical Review A, (1 2015): 0. doi: 10.1103/PhysRevA.91.012305

10/23/2015 72.00 Zeph Landau, Umesh Vazirani, Thomas Vidick. A polynomial time algorithm for the ground state of one-dimensional gapped local Hamiltonians, Nature Physics, (6 2015): 0. doi: 10.1038/nphys3345

10/23/2015 73.00 Beni Yoshida. Topological color code and symmetry-protected topological phases, Physical Review B, (6 2015): 0. doi: 10.1103/PhysRevB.91.245131

10/23/2015 67.00 Jong Yeon Lee, Olivier Landon-Cardinal. Practical variational tomography for critical one-dimensional systems, Physical Review A, (6 2015): 0. doi: 10.1103/PhysRevA.91.062128

10/23/2015 68.00 Fernando Pastawski, Beni Yoshida, Daniel Harlow, John Preskill. Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence, Journal of High Energy Physics, (6 2015): 0. doi: 10.1007/JHEP06(2015)149

10/23/2015 40.00 Mario Berta, Kaushik P. Seshadreesan, Mark M. Wilde. Rényi generalizations of the conditional quantum mutual information, Journal of Mathematical Physics, (02 2015): 0. doi: 10.1063/1.4908102

10/23/2015 41.00 G. Evenbly, G. Vidal. Real-Space Decoupling Transformation for Quantum Many-Body Systems, Physical Review Letters, (6 2014): 0. doi: 10.1103/PhysRevLett.112.220502

10/23/2015 42.00 G. Evenbly, G. Vidal. Theory of minimal updates in holography, Physical Review B, (5 2015): 0. doi: 10.1103/PhysRevB.91.205119

10/23/2015 43.00 Glen Evenbly, Robert N. C. Pfeifer. Improving the efficiency of variational tensor network algorithms, Physical Review B, (6 2014): 0. doi: 10.1103/PhysRevB.89.245118

10/23/2015 44.00 G. Evenbly, G. Vidal. Scaling of entanglement entropy in the (branching) multiscale entanglement renormalization ansatz, Physical Review B, (6 2014): 0. doi: 10.1103/PhysRevB.89.235113

10/23/2015 45.00 G. Vidal, G. Evenbly. Algorithms for Entanglement Renormalization: Boundaries, Impurities and Interfaces, Journal of Statistical Physics, (4 2014): 0. doi: 10.1007/s10955-014-0983-1

10/23/2015 46.00 Philip Richerme, Zhe-Xuan Gong, Aaron Lee, Crystal Senko, Jacob Smith, Michael Foss-Feig, Spyridon Michalakis, Alexey V. Gorshkov, Christopher Monroe. Non-local propagation of correlations in quantum systems with long-range interactions, Nature, (7 2014): 0. doi: 10.1038/nature13450

10/23/2015 47.00 Zhe-Xuan Gong, Michael Foss-Feig, Spyridon Michalakis, Alexey V. Gorshkov. Persistence of Locality in Systems with Power-Law Interactions, Physical Review Letters, (7 2014): 0. doi: 10.1103/PhysRevLett.113.030602

10/23/2015 48.00 Kristan Temme, Fernando Pastawski, Michael J Kastoryano. Hypercontractivity of quasi-free quantum semigroups, Journal of Physics A: Mathematical and Theoretical, (10 2014): 0. doi: 10.1088/1751-8113/47/40/405303

10/23/2015 49.00 Fernando Pastawski, Robert König. Generating topological order: No speedup by dissipation, Physical Review B, (7 2014): 0. doi: 10.1103/PhysRevB.90.045101

10/23/2015 50.00 John Dengis, Robert König, Fernando Pastawski. An optimal dissipative encoder for the toric code, New Journal of Physics, (01 2014): 0. doi: 10.1088/1367-2630/16/1/013023

10/23/2015 51.00 Kristan Temme. Runtime of unstructured search with a faulty Hamiltonian oracle, Physical Review A, (8 2014): 0. doi: 10.1103/PhysRevA.90.022310

10/23/2015 52.00 Peter Brooks, Alexei Kitaev, John Preskill. Protected gates for superconducting qubits, Physical Review A, (5 2013): 0. doi: 10.1103/PhysRevA.87.052306

10/23/2015 53.00 Ning Bao, Patrick Hayden, Grant Salton, Nathaniel Thomas. Universal quantum computation by scattering in the Fermi–Hubbard model, New Journal of Physics, (09 2015): 0. doi: 10.1088/1367-2630/17/9/093028

10/23/2015 54.00 Marco Tomamichel, Mario Berta, Masahito Hayashi. Relating different quantum generalizations of the conditional Rényi entropy, Journal of Mathematical Physics, (08 2014): 0. doi: 10.1063/1.4892761

10/23/2015 56.00 Mario Berta, Patrick J. Coles, Stephanie Wehner. Entanglement-assisted guessing of complementary measurement outcomes, Physical Review A, (12 2014): 0. doi: 10.1103/PhysRevA.90.062127

10/23/2015 57.00 Marco Tomamichel, Volkher B. Scholz, Matthias Christandl, Fabian Furrer, Mario Berta. Position-momentum uncertainty relations in the presence of quantum memory, Journal of Mathematical Physics, (12 2014): 0. doi: 10.1063/1.4903989

10/23/2015 60.00 Kaushik P Seshadreesan, Mario Berta, Mark M Wilde. Rényi squashed entanglement, discord, and relative entropy differences, Journal of Physics A: Mathematical and Theoretical, (10 2015): 0. doi: 10.1088/1751-8113/48/39/395303

10/23/2015 61.00 Aleksander Kubica, Michael E. Beverland. Universal transversal gates with color codes: A simplified approach, Physical Review A, (3 2015): 0. doi: 10.1103/PhysRevA.91.032330

10/23/2015 62.00 Yichen Huang, Xie Chen. Quantum circuit complexity of one-dimensional topological phases, Physical Review B, (5 2015): 0. doi: 10.1103/PhysRevB.91.195143

10/23/2015 63.00 Matthew T. Fishman, Steven R. White. Compression of correlation matrices and an efficient method for forming matrix product states of fermionic Gaussian states, Physical Review B, (8 2015): 0. doi: 10.1103/PhysRevB.92.075132

10/23/2015 64.00 Sergey Bravyi, David Gosset. Gapped and gapless phases of frustration-free spin-12 chains, Journal of Mathematical Physics, (06 2015): 0. doi: 10.1063/1.4922508

10/23/2015 65.00 Simon Forest, David Gosset, Vadym Kliuchnikov, David McKinnon. Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets, Journal of Mathematical Physics, (08 2015): 0. doi: 10.1063/1.4927100

10/23/2015 66.00 Olivier Landon-Cardinal, Beni Yoshida, David Poulin, John Preskill. Perturbative instability of quantum memory based on effective long-range interactions, Physical Review A, (3 2015): 0. doi: 10.1103/PhysRevA.91.032303

TOTAL: 80

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper
05/29/2016 81.00	Spyridon_Michalakis, David_Perez_Garc?a, Norbert_Schuch, J._Ignacio_Cirac. Robustness in projected entangled pair states, Physical Review B (accepted), (09 2013): 115108. doi:
05/29/2016 95.00	Andrew_M._Childs, David_Gosset, Zak_Webb. COMPLEXITY OF THE XY ANTIFERROMAGNET AT FIXED MAGNETIZATION, Quantum Information & Computation, (01 2016): 1. doi:
TOTAL:	**2**

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
05/29/2016 89.00	Marco_Tomamichel, Mario_Berta, Masahito_Hayashi. A duality relation connecting different quantumgeneralizations of the conditional R´enyi entropy, IEEE International Symposium on Information Theory. , . : ,
TOTAL:	**1**

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
05/29/2016	96.00 Anne_Broadbent, Stacey_Jeffery. Quantum Homomorphic Encryption for Circuitsof Low T-gate Complexity, 35th Annual International Cryptology Conference, CRYPTO 2015. , . : ,
10/22/2015	27.00 Bill Fefferman, Ronen Shaltiel, Christopher Umans, Emanuele Viola. On beating the hybrid argument, the 3rd Innovations in Theoretical Computer Science Conference. 07-JAN-12, Cambridge, Massachusetts. : ,
10/23/2015	71.00 Joseph Fitzsimons, Thomas Vidick. A Multiprover Interactive Proof System for the Local Hamiltonian Problem, the 2015 Conference. 11-JAN-15, Rehovot, Israel. : ,
10/23/2015	74.00 Mario Berta, Joseph M. Renes, Mark M. Wilde. Identifying the information gain of a quantum measurement, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,
10/23/2015	75.00 Mario Berta, Omar Fawzi, Volkher Scholz, Oleg Szehr. Variations on classical and quantum extractors, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,
10/23/2015	76.00 Mario Berta, Joseph M. Renes, Mark M. Wilde. Identifying the information gain of a quantum measurement, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,
10/23/2015	77.00 Joseph Fitzsimons, Thomas Vidick. A Multiprover Interactive Proof System for the Local Hamiltonian Problem, the 2015 Conference. 11-JAN-15, Rehovot, Israel. : ,
10/23/2015	39.00 Omar Fawzi, Volkher Scholz, Oleg Szehr, Mario Berta. Variations on classical and quantum extractors, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,
10/23/2015	55.00 Mario Berta, Joseph M. Renes, Mark M. Wilde. Identifying the information gain of a quantum measurement, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,
10/23/2015	58.00 Omar Fawzi, Volkher Scholz, Oleg Szehr, Mario Berta. Variations on classical and quantum extractors, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,
10/23/2015	59.00 Mario Berta, Joseph M. Renes, Mark M. Wilde. Identifying the information gain of a quantum measurement, 2014 IEEE International Symposium on Information Theory (ISIT). 29-JUN-14, Honolulu, HI, USA. : ,

TOTAL: 11

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper
05/29/2016 08.00	Robert_Raussendorf, Dan_E._Browne, Nicolas_Delfosse, Cihan_Okay, Juan_Bermejo-Vega. Contextuality as a resource for qubit quantum computation, ArXiv (11 2015)
05/29/2016 09.00	Mario_Berta, Omar_Fawzi, Volkher_B._Scholz. Quantum Bilinear Optimization, ArXiv (06 2015)
05/29/2016 10.00	Linghang_Kong, Elizabeth_Crosson. The performance of the quantum adiabatic algorithm on spike Hamiltonians, ArXiv (11 2015)
05/29/2016 11.00	Elizabeth_Crosson, Aram_W._Harrow. Simulated Quantum Annealing Can Be Exponentially Faster than Classical Simulated Annealing, ArXiv (01 2016)
05/29/2016 12.00	Anna_Komar, Olivier_Landon-Cardinal, Kristan_Temme. Self correction requires Energy Barrier for Abelian quantum doubles, ArXiv (01 2016)
05/29/2016 05.00	Sergey_Bravyi, David_Gosset. Improved classical simulation of quantum circuits dominated by Cli ord gates, ArXiv (01 2016)
05/29/2016 06.00	Stacey_Jeffery, Shelby_Kimmel. NAND-Trees, Average Choice Complexity, and Effective Resistance, ArXiv (11 2015)
05/29/2016 07.00	Tsuyoshi_Ito, Stacey_Jeffery. Approximate Span Programs, ArXiv (07 2015)
TOTAL:	**8**

Number of Manuscripts:

Books

Received	Book
TOTAL:	

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Mario Berta	1.00
FTE Equivalent:	**1.00**
Total Number:	**1**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
John Preskill	0.02	Yes
Leonard Schulman	0.01	
FTE Equivalent:	**0.03**	
Total Number:	**2**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Final Report
Research on Quantum Algorithms at the Institute for Quantum Information and Matter

Principal Investigators: John Preskill, Leonard Schulman (Caltech)
Other Faculty: Alexei Kitaev, Thomas Vidick (Caltech)
Postdoctoral Associates: Gorjan Alagic, Mario Berta, Elizabeth Crosson, Nicolas Delfosse, Glen Evenbly, Omar Fawzi, David Gossett, Stacey Jeffery, Olivier Landon-Cardinal, Spiros Michalakis, Fernando Pastawski, Kristan Temme, Beni Yoshida
Faculty Associates: Todd Brun (USC), Sandy Irani (UC Irvine)
Graduate Students: Michael Beverland, Peter Brooks, Bill Fefferman, Matt Fishman, Jeongwan Haah, Isaac Kim, Anna Komar, Alex Kubica, Sujeet Shukla, Nicole Yunger Halpern
Type of Award: QA
Start Date: 2012
End Date: 2016
Report Date: May 2016, award ended February 29, 2016

Main Project Goals:
The central goals of our project are (1) to bring large-scale quantum computers closer to realization by proposing and analyzing new schemes for protecting quantum systems from noise, and (2) to conceive, develop, and analyze new applications of quantum computing to physics and mathematics.

Project Description:
This project is devoted to building the theoretical foundations of quantum information science across a broad front, with a particular emphasis on quantum algorithms, quantum complexity, and fault-tolerant quantum computing. Basic advances in all of these areas are needed to bring revolutionary quantum technologies closer to realization. The research is conducted at Caltech's Institute for Quantum Information and Matter (IQIM).

Our research on fault-tolerant quantum computing addresses the crucial questions: How much noise can be tolerated by a quantum computer, and how does the noise impact the resources needed to complete a large-scale computation successfully? It is vital to answer these questions to assess the prospects for realizing powerful quantum technologies. Our approach emphasizes rigorous results. We are also pursuing new ways to encode and process quantum information that are intrinsically robust on physical grounds.

Our research on quantum algorithms emphasizes new applications that reach beyond the hidden subgroup paradigm. Topics of particular interest include algorithms based on tensor contractions and simulations of quantum many-body systems using quantum or classical computers. We hope to sharpen understanding of which simulation problems are hard for classical computers, and to propose interesting simulations that might be achieved using existing methods for controlling physical systems such as cold atoms trapped in optical lattices.

Status and Accomplishments (incomplete list).

Our contributions in 2012-2013 included:
- a scheme for obfuscating quantum circuits,
- a method for performing quantum gates protected by a continuous variable code,
- a proposed quantum resistant cryptosystem based on the hardness of solving systems of quadratic equations,
- a magic state distillation protocol with reduced overhead,
- new connections between quantum information science and quantum many-body physics.

Our contributions in 2013-14 included:
- an algorithm for simulating fermionic quantum field theories using a quantum computer,
- bounds on information propagation rates in quantum systems with long-range interactions,
- efficient dissipative algorithms for preparing topologically encoded quantum states,
- new algorithms for simulating quantum impurity systems using a classical computer.

Our contributions in 2014-15 included:
- a proposed scheme for quantum homomorphic encryption,
- a classification of fault-tolerant logical gates in topological quantum codes,
- circuits for efficient simulation of single-qubit unitary transformations,
- multiprover interactive protocols for verifying low-energy states of local Hamiltonians,
- construction of a novel family of quantum codes with important implications for the study of quantum gravity.

Our contributions in 2015-16 included:
- an improved classical simulation of quantum circuits dominated by Clifford gates,
- a new method for designing quantum algorithms based on span programs,

- a demonstration that quantum simulated annealing can be exponentially faster than classical simulating annealing,
- a proof that the mixing time for abelian quantum double models is independent of system size,
- an accuracy threshold for encoded quantum annealing schemes.

Five graduate students completed their Ph.D. degrees in 2012-2016. Michael Beverland will be awarded his degree in June 2016, and will join Microsoft Research. Peter Brooks joined HRL Laboratories; Bill Fefferman is a Postdoctoral Scholar at the Joint Center for Quantum Information and Computer Science (University of Maryland/NIST); Jeongwan Haah is a Pappalardo Fellow at MIT, and Isaac Kim is a postdoctoral fellow at Perimeter Institute.

Eight postdoctoral scholars moved on from IQIM to faculty or staff positions elsewhere: Gorjan Alagic, Postdoctoral Scholar (University of Copenhagen); Glen Evenbly, Postdoctoral Scholar (UC Irvine); Omar Fawzi, Assistant Professor of Computer Science (ENS de Lyon); David Gosset, Research Staff (IBM T.J. Watson Research Center); Olivier Landon-Cardinal, Postdoctoral Scholar (McGill University); Fernando Pastawski, Postdoctoral Scholar (Freie Universität, Berlin), Kristan Temme, Research Staff (IBM T.J. Watson Research Center); Beni Yoshida, Senior Postdoctoral Researcher (Perimeter Institute).

Here are some highlights of our research accomplishments under this project.

Accomplishments in 2012-13

Quantum circuit obfuscation schemes based on braids [1]:
A circuit obfuscator is an algorithm that translates logic circuits into functionally-equivalent similarly-sized logic circuits that are hard to understand. Circuit obfuscators have obvious practical applications for hiding the design of physical circuits. Sufficiently powerful obfuscators would also have significant theoretical implications in cryptography, such as the ability to turn private-key encryption into public-key encryption. While ad hoc obfuscators exist, theoretical progress has mainly been limited to no-go results. Gorjan Alagic, with Stephen Jordan, proposed a new notion of circuit obfuscation, which they call partial-indistinguishability. They proved that, in contrast to previous definitions of obfuscation, partial-indistinguishability obfuscation can be achieved by a polynomial-time algorithm. Specifically, their algorithm re-compiles the given circuit using a gate that satisfies the relations of the braid group, and then reduces to a braid normal form. A variant of this obfuscation algorithm can also be applied to quantum circuits. Very little is known about quantum circuit obfuscation, and this work appears to be the first nontrivial result in that area.

An MQ/Code Cryptosystem Proposal [19]:
Quantum computers will be able to break public key cryptosystems which are widely used in electronic commerce. How will we protect our privacy against adversaries in a post-quantum world? Are there classical public key cryptosystems that will effectively resist quantum attacks? One proposed scheme, due to McEliece, is based on the hardness of decoding error-correcting codes, but recent successful attacks on the McEliece scheme have called its security into question. Leonard Schulman has proposed a new scheme based on the hardness of solving systems of quadratic equations. Though it is also code-based, in Schulman’s proposal the error-correcting code is not revealed in the public key, which protects against the leading attacks on McEliece's method.

An area law and sub-exponential algorithm for 1D systems [10]:
It has been known for several years that, in the ground state of a one-dimensional quantum system with a local Hamiltonian and an energy gap, the entanglement entropy of a connected subsystem is bounded above by a constant independent of the subsystem’s size. Alexei Kitaev and collaborators showed that this constant scales linearly with the reciprocal of the spectral gap, a big improvement over the best previous estimate, which scaled exponentially. They also found an algorithm for approximating the ground state which runs in subexponential time. These results notably improve our understanding of entanglement in ground states of local quantum systems and of the computational complexity of simulating these systems.

Protected gates based on continuous-variable quantum codes [15]:
How can we protect quantum computers against noise? One way is to use quantum codes and active error correction, another is to control errors passively using braiding of non-abelian anyons. Yet another, performing quantum gates with superconducting circuits, passively protected by continuous variable quantum codes, was analyzed by Peter Brooks, Alexei Kitaev, and John Preskill. In their scheme, gates are executed by turning on and off a tunable Josephson coupling between an LC oscillator and a superconducting qubit or pair of qubits; assuming perfect qubits, they showed that the gate errors are exponentially small when the oscillator's impedance is large in natural units. If superconducting circuits with very high inductance can be achieved experimentally, this scheme suggests a promising route to high-fidelity quantum computing protected by a novel physical encoding of quantum information.

Magic state distillation with low overhead [4]:
Most approaches to fault-tolerant quantum computing use distillation of so-called magic states to achieve a universal set of quantum gates, and distillation dominates the overhead cost of quantum fault tolerance in many such schemes. Jeongwan Haah and Sergey Bravyi proposed a new family of “triorthogonal” error-detecting stabilizer codes that substantially improve the overhead cost of state distillation. Compared to the best previously known protocol, their method reduces the overhead by a

factor of two for distilling magic states with accuracy 10-12.

Fault-tolerant gadgets protected against highly biased noise [16]
Peter Brooks and John Preskill developed a scheme for fault-tolerant quantum computation based on asymmetric Bacon-Shor codes, which works effectively against highly biased noise dominated by dephasing. They found the optimal Bacon-Shor block size as a function of the noise strength and the noise bias, and estimated the logical error rate and overhead cost achieved by this optimal code. Their fault-tolerant gadgets, based on gate teleportation, are well suited for hardware platforms with geometrically local gates in two dimensions.

Sufficient condition on noise correlations for scalable quantum computing [18]:
John Preskill studied the effectiveness of fault-tolerant quantum computation against correlated Hamiltonian noise, and derived a sufficient condition for scalability. He showed that arbitrarily long quantum computations can be executed reliably provided that noise terms acting collectively on k system qubits are sufficiently weak, and decay sufficiently rapidly with increasing k and with increasing spatial separation of the qubits.

A class of highly entangled many-body states that can be efficiently simulated [2]:
Glen Evenbly, with Guifre Vidal, introduced a quantum circuit that produces a highly entangled state of N qubits for which one can efficiently compute expectation values of local observables. Specifically, in a lattice system in D dimensions, the scaling of entanglement of a region of size LD in a state described by this circuit is not subject to restrictions such as a boundary law LD-1, but can be proportional to the volume of the region. They argued that this circuit could be suitable as a variational ansatz for certain classes of highly entangled quantum ground states.

Accomplishments in 2013-14

Quantum algorithms for fermionic quantum field theories [36]:
John Preskill has been working with Jordan and Lee on applications of quantum computing to quantum simulation, in particular the simulation of quantum field theories. Though formally a field theory has an infinite number of degrees of freedom per unit volume, they had shown in previous work that a particle scattering process can be accurately simulated using a number of qubits and quantum gates that scales polynomially with the energy and the number of particles produced in the process. They have recently developed an algorithm for simulating theories with fermions, introducing a variety of new techniques. This work constitutes further progress towards an efficient quantum algorithm for simulating the Standard Model of particle physics.

Persistence of locality in systems with power-law interactions [31, 32]:
Motivated by recent experiments with ultra-cold matter, Spiros Michalakis and collaborators derived a new bound on the propagation of information in D-dimensional lattice models exhibiting long-range interactions. This bound contains two terms: One accounts for the short-ranged part of the interactions, giving rise to a bounded velocity and reflecting the persistence of locality out to intermediate distances, while the other contributes a power-law decay at longer distances. They demonstrated that these two contributions not only bound, but qualitatively reproduce the short- and long-distance dynamical behavior following a local quench in an XY chain and a transverse-field Ising chain. Their results demonstrate that even modestly-sized quantum simulators are well-suited for studying complicated many-body systems that are intractable to classical computation.

Dissipative state preparation [34, 35]:
Fernando Pastawski, with Koenig, has studied the resources needed to prepare many-particle states with long-range entanglement using local dissipative open system dynamics. They showed that a dissipative encoder can prepare a topologically-ordered ground state of a local Hamiltonian on an $L \times L$ lattice in time $O(L)$, which is optimal. This scaling compares favorably with previously known local unitary encoders for the toric code which take time of order $\Omega(L^2)$ and require active time-dependent control. They also proved that for any topological code in D dimensions, the time required to encode logical information into the ground space is at least $\Omega(d1/(D-1))$, where d is the code distance.

A theory of minimal updates in holography [23, 26]:
Glen Evenbly, with Vidal, has advanced the theory of entanglement renormalization, the modern formulation of the real-space renormalization group for quantum systems on a lattice, based on the removal of short-range entanglement in each coarse-graining step. Their work relates tensor network methods to holography, where a many-body system is regarded as the boundary of another system in one higher dimension, with the extra dimension corresponding to renormalization scale. Specifically, they have proposed and applied a theory of minimal updates in holography, answering how much a holographic description of a quantum ground state needs to be modified when the local Hamiltonian of the system is changed in a bounded region. This research sets the stage for applying tensor network methods to problems in holographic field theories and quantum gravity.

Accomplishments in 2014-15

Characterizing fault-tolerant gates in topological quantum codes:
Quantum error-correcting codes protect quantum information from noise, but for scalable quantum computation we also need to

be able to process the encoded quantum data without uncontrolled propagation of error. Preskill, Pastawski, and Yoshida, with student Michael Beverland and other collaborators, classified the logical gates that can be performed on topologically encoded data with manageable error propagation [71,72]. In related work with student Alex Kubica, Pastawski, Yoshida, and Beverland [56,71] worked out explicit mappings between codes, which can be exploited to broaden the family of fault-tolerant operations. These mappings can also be applied to the classification of topological phases of quantum matter.

Quantum Homomorphic Encryption for Circuits of Low T-Gate Complexity:
A fully homomorphic encryption scheme is a method of encryption with the property that any computation on the plaintext can be performed by a party having access to the ciphertext only. The first classical schemes for fully homomorphic encryption were discovered just a few years ago. Postdoc Stacey Jeffery, with Anne Broadbent, has proposed two quantum schemes which are provably secure, but become inefficient for quantum circuits with large complexity [63]. These schemes, the first of their kind, are reminiscent of early classical schemes which applied only to circuits with a limited number of multiplication gates, but turned out to be precursors of efficient fully homomorphic encryption schemes.

Reconstruction of quantum states with small conditional mutual information:
For a quantum state with three disjoint parts A, B, and C, the conditional mutual information (CMI) I(A:C|B) quantifies how strongly A and C are correlated from the viewpoint of an observer in B. In particular, when I(A:C|B) = 0, the full state on ABC can be perfectly reconstructed using an operation mapping B to BC applied to the marginal state on AB; no access to A is needed, because A and C have no surviving correlations once B is completely known. Shortly before his arrival at IQIM, postdoc Omar Fawzi, with Renato Renner, showed that the reconstruction still succeeds with high fidelity when the CMI has a small nonzero value. Since then, this breakthrough result by Fawzi and Renner has been extended in further work by Fawzi and by postdoc Mario Berta, with their collaborators. Sutter, Fawzi, and Renner showed there is a universal recovery map which works on any state with a given marginal on BC [58]. Berta and Tomamichel found an elegant operational proof of the result based on semi-definite programming duality [51]. These results have notable applications to device-independent quantum cryptography, to quantifying entanglement, and to the classification of quantum phases of matter.

Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets:
To run on a fault-tolerant quantum computer, a quantum algorithm needs to be compiled, decomposed in terms of the quantum gates that the computer can execute accurately. A recently constructed compiling algorithm approximates arbitrary single-qubit unitary transformations using the optimal number of gates, but only for the universal gate set consisting of Clifford group gates (symmetries of the octahedron in the Bloch sphere), and one T gate (rotation by angle $\pi/4$). Postdoc David Gosset and collaborators have generalized this construction to the case where the T gate is replaced by a rotation by π/n for particular integer values of n [62]. Such results can significantly reduce the overhead cost of operating a quantum computer.

Spacetime as a quantum error-correcting code:
Two of the most fascinating concepts in physics are quantum error correction (properly encoded quantum states can be protected from damage) and the holographic principle (the information stored in a region of space is subtly encoded on the region's boundary). Recent work by IQIM scientists indicates that these two ideas are more closely related than had been previously appreciated: John Preskill, with postdocs Fernando Pastawski, Beni Yoshida, and Daniel Harlow, constructed quantum error-correcting codes which realize many of the features of the holographic correspondence between a bulk spacetime and its boundary [69]. In particular, local operators deep inside the bulk correspond to highly nonlocal operators on the boundary which are very well protected against errors in which portions of the boundary are erased, and entanglement entropy on the boundary corresponds to geometrical properties of the bulk. In related work, postdoc Ning Bao and collaborators formulated a set of entropy inequalities which characterize the entanglement structure of boundary systems which correspond to smooth bulk geometries [42].

Quantum interactive proofs with entangled provers:
Multiprover quantum interactive proof systems provide a complexity-theoretic lens for studying the nonlocal properties of quantum entanglement. Thomas Vidick, with Joe Fitzsimons, has shown that entanglement shared by a small number of isolated parties can be a surprisingly powerful resource [76]. Specifically, they found a protocol which allows five entangled provers to certify the existence of a low-energy ground state of a local Hamiltonian, by communicating only a constant number of qubits to a verifier; thus the verifier can confirm the existence of a low-energy global n-particle state without being shown more than a constant number of qubits of that state. This result may be a first step towards a multiprover quantum variant of the famous PCP (Probabilistically-Checkable-Proof) Theorem, a cornerstone of classical complexity theory.

Accomplishments in 2015-16

Error correction for encoded quantum annealing. Fernando Pastawski and John Preskill [86] analyzed a quantum annealing architecture recent proposed by Lechner et al., in which a spin glass with all-to-all connectivity is simulated by a spin glass with geometrically local interactions. They pointed out that this scheme is highly robust against measurement errors in the final readout. The simulated spins can be regarded as the logical variables of a classical low-density parity-check code, with a high accuracy threshold.

Improved classical simulation of quantum circuits dominated by Clifford gates. David Gosset, with Sergey Bravyi, considered how the resources needed for classical simulation of a quantum circuit scale with the number t of T gates (rotations by angle ⫽/4), when all the other gates are Clifford gates [87]. Their classical simulation scheme is surprisingly efficient, and may serve as a verification tool for medium-size quantum computations that are dominated by Clifford gates.

Approximate span programs. For any decision problem, there exists a span program leading to an algorithm with optimal quantum query complexity, but finding such an algorithm is generally challenging. Stacey Jeffery, with Tsuyoshi Ito, formulated new ways to design quantum algorithms using span programs [89]. For example, using their techniques, the span program for OR, which can be used to design an optimal algorithm for the OR function, can also be used to design optimal algorithms for threshold functions (in which we want to decide if the Hamming weight of a string is above a threshold or far below, given the promise that one of these is true), and approximate counting (in which we want to estimate the Hamming weight of the input).

Effectiveness of simulated quantum annealing. Simulated quantum annealing is a Monte-Carlo algorithm, running on a classical computer, which samples the equilibrium thermal state of a quantum annealing Hamiltonian. Elizabeth Crosson, with Aram Harrow, showed that simulated quantum annealing sometimes successfully accounts for the effects of quantum tunneling in a quantum annealer, exhibiting an exponential advantage over classical simulated annealing in which quantum tunneling is not faithfully described [93]. This work supports the growing consensus that quantum annealers are unlikely to achieve exponential speedups over classical computing solely by the use of quantum tunneling.

Arrhenius law for mixing time of abelian anyon models. Anna Komar, Olivier Landon-Cardinal, and Kristan Temme studied the mixing times of quantum codes which support abelian anyons described by the group Zd [94]. They showed that these codes have an energy barrier with constant height independent of system size, and that the mixing time follows the Arrhenius law determined by this barrier height. This work provided a rigorous foundation for further explorations of self-correcting quantum memories.

Publications (incomplete list)

[1] G. Alagic, S. Jordan, S. Jeffery, Partial-indistinguishability obfuscation using braids, 21 pages, Proceedings of TQC (2014), arXiv:1212.6458.

[2] G. Evenbly and G. Vidal, A class of highly entangled many-body states that can be efficiently simulated, Phys. Rev. Lett. 112, 240502 (2014), DOI: 10.1103/PhysRevLett.112.240502

[3] B. Fefferman, R. Shaltiel, E. Viola, and C. Umans, On Beating the Hybrid Argument, Theory of Computing Volume 9, Article 26 pp. 809-843 (2013) DOI: 10.4086/toc.2013.v009a026

[4] S. Bravyi and J. Haah, Magic state distillation with low overhead, Phys. Rev. A 86, 052329 (2012), arXiv:1209.2426.

[5] I. H. Kim, Long-range entanglement is necessary for a topological storage of quantum information, Phys. Rev. Lett. 111, 080503 (2013), DOI: 10.1103/PhysRevLett.111.080503

[6] I. H. Kim, Operator extension of strong subadditivity of entropy, J. Math. Phys. 53, 122204 (2012), arXiv:1210.5190.

[7] I. H. Kim, Determining the structure of real-space entanglement spectrum from approximate conditional independence Phys. Rev. B 87, 155120 (2013), arXiv:1210.1831.

[8] I. H. Kim, Perturbative analysis of topological entanglement entropy, Phys. Rev. B 86, 245116 (2012).
[9] I. H. Kim, Long-range entanglement is necessary for a topological storage of quantum information, Phys. Rev. Lett. 111, 080503 (2013), DOI: 10.1103/PhysRevLett.111.080503

[10] I. Arad, A. Kitaev, Z. Landau, and U. Vazirani, An area law and sub-exponential algorithm for 1D systems, arXiv:1301.1162.

[11] T. S. Cubitt, A. Lucia, S. Michalakis, and D. Perez-Garcia, Stability of local quantum dissipative systems, Communications in Mathematical Physics: Volume 337, Issue 3, Page 1275-1315, (2015), DOI: 10.1007/s00220-015-2355-3

[12] M. B. Hastings and S. Michalakis, Quantization of Hall Conductance For Interacting Electrons on a Torus, Commun. Math. Phys., Volume 334, Issue 1, pp. 433-471, (2015). DOI: 10.1007/s00220-014-2167-x

[13] J. Haegeman, S. Michalakis, B. Nachtergaele, T. J. Osborne, N. Schuch, and F. Verstraete, Elementary excitations in gapped quantum spin systems, Phys. Rev. Lett. 111, 080401 (2013), DOI: 10.1103/PhysRevLett.111080401

[14] J. I. Cirac, S. Michalakis, D. Perez-Garcia, and N. Schuch, Robustness in Projected Entangled Pair States, Phys. Rev. B

88, 115108 (2013), DOI: 10.1103/PhysRevB.88.115108

[15] P. Brooks, A. Kitaev, and J. Preskill, Protected gates for superconducting qubits, Phys. Rev. A 87, 052306 (2013), arXiv: 1302.4122.

[16] P. Brooks and J. Preskill, Fault-tolerant quantum computation with asymmetric Bacon-Shor codes, Phys. Rev. A 87, 032310 (2013), arXiv:1211.1400.

[17] J. Napp and J. Preskill, Optimal Bacon-Shor codes, Quant. Inf. Comput. 13, 490-510 (2013), arXiv:1207.6131. http: //resolver.caltech.edu/CaltechAUTHORS:20130325-085516990

[18] J. Preskill, Sufficient condition on noise correlations for scalable quantum computing, Quant. Inf. Comput. 13, 181-194 (2013), arXiv:1207.6131. http://resolver.caltech.edu/CaltechAUTHORS:20130321-160602027

[19] L. Schulman, An MQ/Code Cryptosystem Proposal, Cryptology ePrint Archive: Report 2013/135 (posted 6 Mar 2013, http: //eprint.iacr.org/2013/135).

[20] Mario Berta, Omar Fawzi, Volkher B. Scholz, Oleg Szehr, Variations on Classical and Quantum Extractors, arXiv: 1402.3279 (2014), at IEEE ISIT 2014.

[21] Mario Berta, Kaushik P. Seshadreesan, Mark M. Wilde, Renyi generalizations of the conditional quantum mutual information, Journal of Mathematical Physics vol. 56, no. 2, article no. 022205 (2015). DOI: 10.1063/1.4908102

[22] G. Evenbly and G. Vidal, A real space decoupling transformation for quantum many-body systems, Phys. Rev. Lett. 112, 220502 (2014).

[23] G. Evenbly and G. Vidal, A theory of minimal updates in holography, Phys. Rev. B 91, 205119 (2015). DOI: 10.1103 /PhysRevB.91.205119

[24] G. Evenbly and R. N. C. Pfeifer, Improving the efficiency of variational tensor network algorithms, Phys. Rev. B 89, 245118 (2014).

[25] G. Evenbly and G. Vidal, Scaling of entanglement entropy in the (branching) multi-scale entanglement renormalization ansatz, Phys. Rev. B 89, 235113 (2014).

[26] G. Evenbly and G. Vidal, Algorithms for entanglement renormalization: boundaries, impurities and interfaces, J Stat Phys 157:931-978 (2014). DOI: 10.1007/s10955-014-0983-1

[27] A. Kubica and B. Yoshida, Precise estimation of critical exponents from real-space renormalization group analysis, arXiv: 1402.0619 (2014).

[28] B. Yoshida and A. Kubica Quantum criticality from Ising model on fractal lattices, arXiv:1404.6311 (2014).

[29] Matthew B. Hastings, Spyridon Michalakis, Quantization of Hall Conductance For Interacting Electrons on a Torus, Commun. Math. Phys., Volume 334, Issue 1, pp. 433-471, (2015). DOI: 10.1007/s00220-014-2167-x

[30] J.I. Cirac, S. Michalakis, D. Perez-Garcia, N. Schuch, Robustness in projected entangled pair states, Phys. Rev. B 88, 115108 (2013), arXiv:1306.4003 http://resolver.caltech.edu/CaltechAUTHORS:20131004-092235258

[31] Philip Richerme, Zhe-Xuan Gong, Aaron Lee, Crystal Senko, Jacob Smith, Michael Foss-Feig, Spyridon Michalakis, Alexey V. Gorshkov, Christopher Monroe, Non-local propagation of correlations in long-range interacting quantum systems, Nature 511, 198 (2014). DOI 10.1038/nature13450 http://resolver.caltech.edu/CaltechAUTHORS:20140811-093227563

[32] Zhe-Xuan Gong, Michael Foss-Feig, Spyridon Michalakis, Alexey V. Gorshkov, Persistence of locality in systems with power-law interactions, Phys. Rev. Lett. 113, 030602 (2014). DOI 10.1103/PhysRevLett.113.030602

[33] K. Temme, F. Pastawski, M. J. Kastoryano, Hypercontractivity of quasi-free quantum semigroups, Journal of Physics A: Mathematical and Theoretical, Volume 47, Number 40 (2014). DOI 10.1088/1751-8113/47/40/405303

[34] R Koenig and F Pastawski, Generating topological order: no speedup by dissipation, Phys. Rev. B 90, 045101 (2014). DOI 10.1103/PhysRevB.90.045101

[35] J. Dengis, R. König, and F. Pastawski, An optimal dissipative encoder for the toric code, New Journal of Physics 16 (1),

013023 (2014).

[36] Stephen P. Jordan, Keith S. M. Lee, and John Preskill Quantum Algorithms for Fermionic Quantum Field Theories, arXiv: 1404.7115 (2014).

[37] Kristan Temme, Runtime of unstructured search with a faulty Hamiltonian oracle, Phys. Rev. A 90, 022310 (2014). DOI 10.1103/PhysRevA.90.022310

[38] Beni Yoshida, Violation of the Arrhenius law below the transition temperature, arXiv:1404.0457 (2014).

[39] Ning Bao, Nicole Yunger Halpern, Quantum voting and violation of Arrow's Impossibility Theorem, arXiv:1501.00458.

[40] Ning Bao, ChunJun Cao, Sean M. Carroll, Aidan Chatwin-Davies, Nicholas Hunter-Jones, Jason Pollack, Grant N. Remmen, Consistency conditions for an AdS/MERA Correspondence, arXiv:1504.06632

[41] Ning Bao, Patrick Hayden, Grant Salton, Nathaniel Thomas, Universal Quantum Computation By Scattering in the Fermi-Hubbard Model, arXiv: 1409.3585

[42] Ning Bao, Sepehr Nezami, Hirosi Ooguri, Bogdan Stoica, James Sully, Michael Walter, (2015) The Holographic Entropy Cone. Journal of High Energy Physics, 2015 (9). Art. No. 130. ISSN 1126-6708. http://resolver.caltech.edu/CaltechAUTHORS: 20150616-154806338

[43] Marco Tomamichel, Mario Berta, Masahito Hayashi, Relating different quantum generalizations of the conditional Renyi entropy, J. Math. Phys. 55 (8), 082206 (2014).

[44] Mario Berta, Joseph M. Renes, Mark M. Wilde, Identifying the Information Gain of a Quantum Measurement, IEEE Trans. on Inf. Th., vol. 60, no. 12, p. 7987-8006, 2014.

[45] Mario Berta, Patrick J. Coles, Stephanie Wehner, An equality between entanglement and uncertainty, Phys. Rev. A 90, 062127 (2014).

[46] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B. Scholz, Matthias Christandl, Position-Momentum Uncertainty Relations in the Presence of Quantum Memory, J. Math. Phys. 55, 122205 (2014).

[47] Mario Berta, Omar Fawzi, Volkher B. Scholz, Oleg Szehr, Variations on Classical and Quantum Extractors, ISIT IEEE Int. Symp. on (2014), p. 1474 – 1478.

[48] Mario Berta, Joseph M. Renes, Mark M. Wilde, Identifying the Information Gain of a Quantum Measurement, ISIT IEEE Int. Symp. on (2014), p. 331- 335.

[49] Marco Tomamichel, Mario Berta, Masahito Hayashi, A Duality Relation Connecting Different Quantum Generalizations of the Conditional Rényi Entropy, ISIT IEEE Int. Symp. on (2014), p. 731 – 735.

[50] Marco Tomamichel, Mario Berta, Joseph M. Renes, Quantum Coding with Finite Resources, Nature Communications 7: 11419 10.1038/ncomms11419 (2016)

[51] Mario Berta, Marco Tomamichel (2016) The Fidelity of Recovery Is Multiplicative. IEEE Transactions on Information Theory, 62 (4). pp. 1758-1763. ISSN 0018-9448. http://resolver.caltech.edu/CaltechAUTHORS:20160425-151717984

[52] Mario Berta, Marius Lemm, Mark M. Wilde, (2015) Monotonicity of quantum relative entropy and recoverability. Quantum Information and Computation, 15 (15-16). pp. 1333-1354. ISSN 1533-7146. http://resolver.caltech.edu/CaltechAUTHORS: 20160301-081841151

[53] Kaushik P. Seshadreesan, Mario Berta, Mark M. Wilde, (2015) Rényi squashed entanglement, discord, and relative entropy differences Journal of Physics A: Mathematical and Theoretical, Volume 48, Number 39. DOI 10.1088/1751-8113/48/39/395303

[54] Mario Berta, Matthias Christandl, Dave Touchette, Smooth Entropy Bounds on One-Shot Quantum State Redistribution. IEEE Transactions on Information Theory, 62 (3). pp. 1425-1439. ISSN 0018-9448. http://resolver.caltech. edu/CaltechAUTHORS:20160216-131540447

[55] Mario Berta, Omar Fawzi, Volkher B. Scholz, Quantum-proof randomness extractors via operator space theory, arXiv: 1409.3563.

[56] Aleksander Kubica, Michael E. Beverland, (2015) Universal transversal gates with color codes: A simplified approach. Physical Review A, 91 (3). Art. No. 032330. ISSN 1050-2947. http://resolver.caltech.edu/CaltechAUTHORS:20150501-072926649

[57] Yichen Huang, Xie Chen, (2015) Quantum circuit complexity of one-dimensional topological phases. Physical Review B, 91 (19). Art. No. 195143. ISSN 1098-0121. http://resolver.caltech.edu/CaltechAUTHORS:20150618-130311270

[58] David Sutter, Omar Fawzi, Renato Renner, (2015) Universal recovery map for approximate Markov chains, Proc. R. Soc. A 472: 20150623. http://dx.doi.org/10.1098/rspa.2015.0623

[59] Matthew T. Fishman, Steven R. White, Compression of Correlation Matrices and an Efficient Method for Forming Matrix Product States of Fermionic Gaussian States, arXiv:1504.07701.

[60] Andrew Childs, David Gosset, Zak Webb, (2016) Complexity of the XY antiferromagnet at fixed magnetization. Quantum Information & Computation 16(1&2): 1-18.

[61] Sergey Bravyi, David Gosset, (2015) Gapped and gapless phases of frustration-free spin-1/2 chains Journal of Mathematical Physics 56, 061902. http://dx.doi.org/10.1063/1.4922508

[62] Simon Forest, David Gosset, Vadym Kliuchnikov, David McKinnon, (2015) Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets Journal of Mathematical Physics 56, 082201 10.1063/1.4927100

[63] Anne Broadbent and Stacey Jeffery, Quantum Homomorphic Encryption for Circuits of Low T-Gate Complexity, In: Advances in Cryptology. Lecture Notes in Computer Science. No.9216. Springer , Berlin, pp. 609-629. ISBN 978-3-662-47999-5 http://resolver.caltech.edu/CaltechAUTHORS:20150521-152945536

[64] Olivier Landon-Cardinal, Beni Yoshida, David Poulin, John Preskill, Can long-range interactions stabilize quantum memory at nonzero temperature?, Phys. Rev. A 91, 032303 (2015).

[65] Jong Yeon Lee, Olivier Landon-Cardinal, (2015) Practical variational tomography for critical one-dimensional systems. Physical Review A, 91 (6). Art. No. 062128. ISSN 1050-2947. http://resolver.caltech.edu/CaltechAUTHORS:20150724-074526381

[66] Fernando Brandao, Toby Cubitt, Angelo Lucia, Spyridon Michalakis, David Perez-Garcia, Area law for fixed points of rapidly mixing dissipative quantum systems, arXiv:1505.02776.

[67] Angelo Lucia, Toby S. Cubitt, Spyridon Michalakis, David Pérez-García , Rapid mixing and stability of quantum dissipative systems, Phys. Rev. A 91, 040302 (2015). http://resolver.caltech.edu/CaltechAUTHORS:20150501-075446387

[68] Kristan Temme, Fernando Pastawski, Michael J. Kastoryano, Hypercontractivity of quasi-free quantum semigroups, Journal of Physics A:
Mathematical and Theoretical, 47(40), 405303 (2015).

[69] Fernando Pastawski, Beni Yoshida, Daniel Harlow, John Preskill, (2015) Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence. Journal of High Energy Physics, 2015 (6). Art. No. 149. ISSN 1029-8479. http://resolver.caltech.edu/CaltechAUTHORS:20150717-122900464

[70] Aleksander Kubica, Beni Yoshida, Fernando Pastawski, (2015) Unfolding the color code. New Journal of Physics, 17 (8). Art. No. 083026. ISSN 1367-2630. http://resolver.caltech.edu/CaltechAUTHORS:20151001-082745067

[71] Fernando Pastawski, Beni Yoshida, Fault-tolerant logical gates in quantum error-correcting codes. Physical Review A, 91 (1), No. 012305. http://resolver.caltech.edu/CaltechAUTHORS:20150309-111410905

[72] Michael E. Beverland, Oliver Buerschaper, Robert Koenig, Fernando Pastawski, John Preskill, Sumit Sijher, Protected gates for topological quantum field theories. Journal of Mathematical Physics, 57 (2). Art. No. 022201. ISSN 0022-2488. http://resolver.caltech.edu/CaltechAUTHORS:20141209-131847639.

[73] Kristan Temme, Michael J. Kastoryano, How fast do stabilizer Hamiltonians thermalize? arXiv:1505.07811.

[74] Toby Cubitt, Michael Kastoryano, Ashley Montanaro, Kristan Temme, (2015) Quantum reverse hypercontractivity. Journal of Mathematical Physics, 56 (10). Art. No. 102204. ISSN 0022-2488. http://resolver.caltech.edu/CaltechAUTHORS:20151201-094310055

[75] Kristan Temme, Thermalization time bounds for Pauli stabilizer Hamiltonians, arXiv:1412.2858.

[76] Joseph Fitzsimons, Thomas Vidick, A multiprover interactive proof system for the local Hamiltonian problem, arXiv: 1409.0260, Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS '15

[77] Rotem Arnon-Friedman, Renato Renner, Thomas Vidick, Non-signalling parallel repetition using de Finetti reductions, arXiv:1411.1582.

[78] Zeph Landau, Umesh Vazirani, Thomas Vidick , A polynomial time algorithm for the ground state of one-dimensional gapped local Hamiltonians, Nature Physics (1 June 2015), doi:10.1038/nphys3345 http://resolver.caltech.edu/CaltechAUTHORS:20150702-112319520

[79] Beni Yoshida, (2015) Topological color code and symmetry-protected topological phases. Physical Review B, 91 (24). Art. No. 245131. ISSN 1098-0121. http://resolver.caltech.edu/CaltechAUTHORS:20150706-143013854

[80] N. Yunger Halpern, A. J. P. Garner, O. C. O. Dahlsten, and V. Vedral, (2015) What's the worst that could happen? One-shot dissipated work from Rényi divergences. . (Submitted) http://resolver.caltech.edu/CaltechAUTHORS:20150622-113733758

[81] O. C. O. Dahlsten, A. J. P. Garner, M.-S. Choi, D. Braun, N. Yunger Halpern, and V. Vedral, Equality for worst-case work at any protocol speed, arXiv:1504.05152.

[82] N. Yunger Halpern, Beyond heat baths II: Framework for generalized thermodynamic resource theories, arXiv:1409.7845.

[83] N. Yunger Halpern and J. P. Renes, Beyond heat baths: Generalized resource theories for small-scale thermodynamics. Physical Review E, 93 (2). Art. No. 022126. ISSN 2470-0045. http://resolver.caltech.edu/CaltechAUTHORS:20160315-161221220

[84] N. Yunger Halpern, O. C. O. Dahlsten, A. J. P. Garner, and V. Vedral, Unification of fluctuation theorems and one-shot statistical mechanics, arXiv:1409.3878.

[85] G. Gour, M. Mueller, V. Narasimhachar, R. W. Spekkens, and N. Yunger Halpern, (2015) The resource theory of informational nonequilibrium in thermodynamics. Physics Reports, 583 . pp. 1-58. ISSN 0370-1573. http://resolver.caltech.edu/CaltechAUTHORS:20150807-085226114

[86] F. Pastawski and J. Preskill, Error correction for encoded quantum annealing, Phys. Rev. A 93, 052325 (2016). http://resolver.caltech.edu/CaltechAUTHORS:20160525-143009202

[87] S. Bravyi and D. Gosset, Improved classical simulation of quantum circuits dominated by Clifford gates, arXiv:1601.07601.

[88] S. Jeffery and S. Kimmel, NAND-trees, average choice complexity, and effective resistance, arXiv:1511.02235.

[89] T. Ito and S. Jeffery, Approximate span programs, arXiv:1507.00432.

[90] R. Raussendorf, D. E. Browne, N. Delfosse, C. Okay, and J. Bermejo-Vega, Contextuality as a resource for qubit quantum computation, arXiv:1511.08506.

[91] M. Berta, O. Fawzi, and V. B. Scholz, Quantum bilinear optimization, arXiv:1506.08810. http://resolver.caltech.edu/CaltechAUTHORS:20151015-102844005

[92] L. Kong and E. Crosson, The performance of the quantum adiabatic algorithm on spike Hamiltonians, arXiv:1511.06991.

[93] E. Crosson and A. W. Harrow, Simulated quantum annealing can be exponentially faster than classical simulated annealing, arXiv:1601.03030.

[94] A. Komar, O. Landon-Cardinal, and K. Temme, Self correction requires energy barrier for abelian quantum doubles, arXiv: 1601.01324.

Technology Transfer