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

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.
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)

<table>
<thead>
<tr>
<th>Received</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/26/16</td>
<td>78.00 John_Napp, John_Preskill. Optimal Bacon-Shor codes, Quantum Information and Computation, (05 2013): 490. doi:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>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:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>04.00 Fernando_Pastawski, John_Preskill. Error correction for encoded quantum annealing, PHYSICAL REVIEW A, (05 2016): 52325. doi:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>03.00 Gilad_Goura, Markus_P._Müller, Varun_Narasimhachara, Robert_W._Spekkens, Nicole_Yunger_Halpern. The resource theory of informational nonequilibrium inthermodynamics, Physics Reports, (07 2015): 1. doi:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>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:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>01.00 Toby_Cubitt, Michael_Kastoryano, Ashley_Montanaro, Kristan_Temme. Quantum reverse hypercontractivity, Journal of Mathematical Physics, (10 2015): 102204. doi:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>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:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>99.00 Fernando_Pastawski, Beni_Yoshida. Fault-tolerant logical gates in quantum error-correcting codes, PHYSICAL REVIEW A, (01 2015): 12305. doi:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>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:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>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:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>94.00 David_Sutter, Omar_Fawzi, Renato_Renner. Universal recovery map forapproximate Markov chains, Royal Society, (01 2016): 20150623. doi:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>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:</td>
</tr>
<tr>
<td>05/29/16</td>
<td>92.00 Mario_Berta, Marius_Lemmy, Mark_M._Wilde. Monotonicity of quantum relative entropy and recoverability, Quantum Information &amp; Computation, (11 2015): 1333. doi:</td>
</tr>
</tbody>
</table>
Mario Berta, Marco Tomamichel. The Fidelity of Recovery Is Multiplicative, IEEE Transaction on Information Theory, (04 2016): 1758. doi:

Marco Tomamichel, Mario Berta, Joseph M. Renes. Quantum coding with finite resources, Nature Communications, (05 2016): 11419. doi:

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:

Mario Berta, Patrick Coles, Stephanie Wehner. Entanglement-assisted guessing of complementary measurement outcomes, PHYSICAL REVIEW A , (12 2014): 62127. doi:


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:


John Preskill. SUFFICIENT CONDITION ON NOISE CORRELATIONSFOR SCALABLE QUANTUM COMPUTING, Quant. Inf. Comput, (03 2013): 181. doi:


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


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


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


<table>
<thead>
<tr>
<th>Date</th>
<th>Author(s)</th>
<th>Title</th>
<th>Journal/Volume/Publication Details</th>
<th>DOI</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/23/2015</td>
<td>Marco Tomamichel, Mario Berta, Masahito Hayashi</td>
<td>Relating different quantum generalizations of the conditional Rényi entropy</td>
<td>Journal of Mathematical Physics, (08 2014): 0</td>
<td>10.1063/1.4892761</td>
</tr>
</tbody>
</table>

**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 quantum generalizations of the conditional R’enyi entropy, IEEE International Symposium on Information Theory. , , ,

TOTAL:  1
<table>
<thead>
<tr>
<th>Received</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/22/2015 27.00</td>
<td>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.</td>
</tr>
<tr>
<td>10/23/2015 74.00</td>
<td>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.</td>
</tr>
<tr>
<td>10/23/2015 75.00</td>
<td>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.</td>
</tr>
<tr>
<td>10/23/2015 76.00</td>
<td>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.</td>
</tr>
<tr>
<td>10/23/2015 77.00</td>
<td>Joseph Fitzsimons, Thomas Vidick. A Multiprover Interactive Proof System for the Local Hamiltonian Problem, the 2015 Conference. 11-JAN-15, Rehovot, Israel.</td>
</tr>
<tr>
<td>10/23/2015 55.00</td>
<td>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.</td>
</tr>
<tr>
<td>10/23/2015 59.00</td>
<td>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.</td>
</tr>
</tbody>
</table>

**TOTAL:** 11
**Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):**

**(d) Manuscripts**

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

**TOTAL:** 8

**Number of Manuscripts:**

**Books**

<table>
<thead>
<tr>
<th>Received</th>
<th>Book</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TOTAL:**
# Patents Submitted

# Patents Awarded

# Awards

## Graduate Students

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTE Equivalent:</td>
<td>1.00</td>
</tr>
<tr>
<td>Total Number:</td>
<td>1</td>
</tr>
</tbody>
</table>

## Names of Post Doctorates

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mario Berta</td>
<td>1.00</td>
</tr>
<tr>
<td>FTE Equivalent:</td>
<td>1.00</td>
</tr>
<tr>
<td>Total Number:</td>
<td>1</td>
</tr>
</tbody>
</table>

## Names of Faculty Supported

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
<th>National Academy Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Preskill</td>
<td>0.02</td>
<td>Yes</td>
</tr>
<tr>
<td>Leonard Schulman</td>
<td>0.01</td>
<td></td>
</tr>
<tr>
<td>FTE Equivalent:</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>Total Number:</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

## Names of Under Graduate students supported

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTE Equivalent:</td>
<td></td>
</tr>
<tr>
<td>Total Number:</td>
<td></td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>NAME</th>
<th>Total Number:</th>
</tr>
</thead>
</table>

**Names of personnel receiving PHDs**

<table>
<thead>
<tr>
<th>NAME</th>
<th>Total Number:</th>
</tr>
</thead>
</table>

**Names of other research staff**

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>FTE Equivalent:</th>
<th>Total Number:</th>
</tr>
</thead>
</table>

**Sub Contractors (DD882)**

**Inventions (DD882)**
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
Quantum error-correcting codes protect quantum information from noise, but for scalable quantum computation we also need to characterize fault-tolerant gates in topological quantum codes:

Accomplishments in 2014-15

Gravity.

A critical step is understanding how the 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.

Specifically, they have proposed and applied a theory of minimal updates in holography, answering how much a holographic boundary of another system in one higher dimension, with the extra dimension corresponding to renormalization scale.

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 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 renormalization group for quantum systems on a lattice, based on the removal of short-range entanglement in each coarse-graining step. This bound contains two terms:

A theory of minimal updates in holography [23, 26]:

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 × 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 \( \Omega(d/(D-1)) \), 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 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 × 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 \( \Omega(d/(D-1)) \), 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 $\pi/n$ 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 $\pi/4$), 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 $\mathbb{Z}_d$ [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)


[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


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


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


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


Technology Transfer