Curriculum Vitae

Gregory D. Kahanamoku-Meyer, PhD

maiden name: Gregory D. Meyer

cell: (802) 922-1876
email: gkm@berkeley.edu
website: https://gregkm.me/

Summary

I am a researcher who bridges computer science and quantum physics, with a focus on bringing theoretical ideas to practical realization. I design algorithms and cryptographic protocols for quantum computers, specifically targeting current or near-term quantum devices. I also develop high-performance computing tools for discovering and engineering new physics.

Academic History

JAN 2024 - PRESENT

Massachusetts Institute of Technology - *Postdoctoral Associate*

- Labs of Dr. Isaac Chuang and Dr. Peter Shor

JULY 2023 - JAN 2024

Lawrence Berkeley National Laboratory + **UC Berkeley** - *Postdoctoral Researcher*

AUGUST 2017 - JUNE 2023

University of California at Berkeley - *PhD, Physics*

- Advisor: Dr. Norman Yao (Physics, now at Harvard Physics)
- Co-advised by Dr. Umesh Vazirani (Electrical Engineering and Computer Science)
- Master's degree awarded 2019

SUMMER 2021, SUMMER 2023

Simons Institute for the Theory of Computing - *Visiting Researcher*

OCTOBER 2016 - JULY 2017

University of California at Berkeley - *Post-baccalaureate Researcher*

AUGUST 2012 - MAY 2016

Yale University - *Bachelor of Science, Physics (intensive track)*

- Distinction in the major
- Cum laude

SUMMER 2015

National Institute of Standards and Technology (NIST), Time and Frequency Division - *Summer Undergraduate Research Fellow*

SUMMER 2013 - MAY 2015

European Organization for Nuclear Research (CERN), ATLAS collaboration – *Undergraduate Researcher*

Fellowships, Grants, and Awards

2018-2021

National Defense Science & Engineering Graduate Fellowship (NDSEG) – *US Department of Defense*
$115,200 stipend over three years, plus tuition, fees, etc.

2018 (declined for NDSEG above)

Graduate Research Fellowship Program (GRFP) – *US National Science Foundation*
$102,000 stipend over three years, plus tuition, fees, and institutional grant

2017-2018

Heising-Simons Fellowship in Physics – *University of California at Berkeley*
$67,000 for first year of PhD tuition and stipend + $1,500 bonus each succeeding year

2017-2023

National Energy Research Scientific Computing Center (NERSC) Grants – *US Department of Energy*
Awarded allocations of compute time on the NERSC supercomputer, for the study of many-body quantum physics and its relationship to theories of quantum gravity. (Co-written with colleagues).

2016

Howard L. Schultz Award – *Yale University*
$1,000. Awarded at commencement by the Yale Physics department for "excellence, inventiveness, and good taste in experimental physics"

2015

Summer Undergraduate Research Fellowship – *National Institute of Standards and Technology (NIST), Yale University*
$9,100. In support of research at NIST in Boulder, CO

2014

Alan S. Tetelman 1958 Fellowship; Yale Science Scholars Program – *Yale University*
$4,500. In support of research at CERN in Geneva, Switzerland

2013

Alan S. Tetelman 1958 Fellowship – *Yale University*
$7,000. In support of research at CERN in Geneva, Switzerland

Research

My research focuses on the intersections of three broad topics: quantum physics, cryptography, and high performance computing. In graduate school and my postdoctoral studies, this has included the following research projects:

Classically-verifiable quantum computational advantage

Tests of quantum computational advantage seek to demonstrate the power of quantum computers by performing computations that are infeasible for even the top classical supercomputers. But the tests that have been performed thus far are equally hard to *check*. Much of my PhD work focused on tests of quantum computational advantage that are efficiently verifiable by classical computers, while still remaining hard to spoof. My results include breaking the security of a test protocol that had stood for over a decade, creating a new protocol that is provably secure under standard hardness assumptions, helping experimentally implement a proof-of-concept demonstration of that protocol, and exploring further applications of these protocols in quantum cryptography.

Massively parallel numerical quantum dynamics

Numerical study has proven to be one of the core tools for exploring the emergent properties of many-body quantum systems. I am the primary author of the `dynamite` library, which provides extremely fast time evolution and eigensolving for numerical quantum many-body spin chain physics, parallelized using MPI and GPU acceleration. I also have worked with the Scalable Solvers Group at Lawrence Berkeley National Laboratory on applying cutting edge numerical linear algebra techniques in hybrid OpenMP-MPI as well as GPU accelerated settings. I performed most of my work using the Department of Energy's NERSC supercomputer, and Harvard University's compute cluster.

Fast circuits for quantum multiplication

Multiplication of superpositions of integers is a crucial operation for cryptographically-relevant quantum algorithms such as Shor's algorithm for factoring. I designed a new algorithm for quantum multiplication that outperforms long-standard techniques, achieving a gate count that is asymptotically sub-quadratic in the length of the inputs while only using a small constant number of ancilla qubits.

GPU-accelerated post-quantum cryptanalysis

I wrote the first (to my knowledge) GPU accelerated implementation of Dumer's algorithm for breaking the Learning Parity with Noise (LPN) problem, whose hardness assumption is a major candidate for post-quantum cryptography schemes. For over a year I held a world record in Inria's online competition.

Undergraduate Research

As an undergraduate I undertook the following research projects:

2015-2016
Quantum control of qubit-cavity systems (advisor: Dr. Liang Jiang, Yale)

2015
Characterization and tuning of atomic clocks (advisor: Dr. Joshua Savory, NIST)

2013-2015
Experimental high-energy particle physics (advisors: Dr. Tobias Golling, Yale; Dr. Till Eifert, CERN; Dr. Ben Nachman, CERN)

2014-2016
Microgravity scientific tool design (Yale Drop Team, advisor: Dr. Stephen Irons, Yale)

Programming

Author of popular open source packages (link to GitHub):

- **`dynamite`**: massively parallel numerical analysis of quantum many-body spin systems
- **IT8951**: driver for the IT8951 e-paper controller in embedded systems

Languages
Python, C, C++: 10 years experience
Julia: 4 years experience

Tools
Cython, MPI, OpenMP, CUDA: 7 years experience
Containerization (Docker/Podman, in HPC settings via Singularity and Shifter): 2 years experience

Publications

* = co-first authorship

10. **G. Kahanamoku-Meyer**, N. Yao. **Fast quantum integer multiplication with zero ancillas.** arXiv:2403:18006

9. **G. Kahanamoku-Meyer**. **Forging quantum data: classically defeating an IQP-based quantum test.** Quantum 7, 1107 (2023)

8. Z. Brakerski, A. Gheorghiu, **G. Kahanamoku-Meyer**, E. Porat, T. Vidick. **Simple Tests of Quantumness Also Certify Qubits.** CRYPTO 2023

7. ***G. Kahanamoku-Meyer**, *D. Zhu, L. Lewis, C. Noel, O. Katz, B. Harraz, Q. Wang, A. Risinger, L. Feng, D. Biswas, L. Egan, A. Gheorghiu, Y. Nam, T. Vidick, U. Vazirani, N. Yao, M. Cetina, C. Monroe.

Interactive cryptographic proofs of quantumness using mid-circuit measurements. Nat. Phys. 19, 1725–1731 (2023)

6. **G. Kahanamoku-Meyer**, S. Choi, U. Vazirani, N. Yao. **Classically-verifiable quantum advantage from a computational Bell test.** Nat. Phys. 18, 918–924 (2022)

5. R. Van Beeumen, K. Ibrahim, **G. Kahanamoku-Meyer**, N. Yao, C. Yang. **Enhancing scalability of a matrix-free eigensolver for studying many-body localization.** The International Journal of High Performance Computing Applications, 36(3), 307–319 (2022)

4. B. Kobrin, Z. Yang, **G. Kahanamoku-Meyer**, C. Olund, J. Moore, D. Stanford, N. Yao. **Many-Body Chaos in the Sachdev-Ye-Kitaev Model.** Phys. Rev. Lett. 126, 030602 (2021)

3. F. Machado, D. Else, **G. Kahanamoku-Meyer**, C. Nayak, N. Yao. **Long-Range Prethermal Phases of Nonequilibrium Matter.** Phys. Rev. X 10, 011043 (2020)

2. R. Van Beeumen, **G. Kahanamoku-Meyer**, N. Yao, C. Yang. **A scalable matrix-free iterative eigensolver for studying many-body localization.** HPCAsia2020: Proceedings of the International Conference on High Performance Computing in Asia-Pacific Region (2020)

1. F. Machado, **G. Kahanamoku-Meyer**, D. Else, C. Nayak, N. Yao. **Exponentially Slow Heating in Short and Long-range Interacting Floquet Systems.** Phys. Rev. Research 1, 033202 (2019)

Seminars and other talks

2023-11-02, University of Hawai'i at Mānoa, Department of Physics and Astronomy. *Department colloquium*.

2023-10-26, Google Quantum AI. *Guest seminar*.

2023-10-25, Caltech Institute for Quantum Information and Matter. *IQIM seminar*.

2023-10-20, Massachusetts Institute of Technology. *Quantum information science group seminar*.

2023-10-19, Harvard University. *Quantum information seminar*.

2023-07-14, Simons Institute for the Theory of Computing, Summer Cluster Workshop. *Lightning talk*.

2023-03-01, IBM Quantum. *Guest seminar*.

2022-08-04, CLEAR Project. *PubScience*.

2022-05-03, UC Berkeley. *Guest lecture, CHEM 195/295: Special topics in Quantum Computing*.

2022-03-15, APS March Meeting. *Quantum Digital and Analog Algorithms [Focus]*. (invited)

2022-02-22, Harvard University, Department of Physics. *CMT Kid's Seminar*.

2022-02-09, Quantum Systems Accelerator (QSA). *Science session*.

2021-11-10, IBM Quantum. *Quantum computing seminar*.

2021-10-08, MIT Cryptography and Information Security group. *CIS seminar*.

2021-09-29, NSF Challenge Institute for Quantum Computation (CIQC). *Colloquium introduction*.

2021-09-28, Physics of Information and Quantum Technologies, IT Lisbon. *Group meeting*.

2021-07-14, Simons Institute for the Theory of Computing. *Quantum Wave in Computing Reunion*.

2021-05-21, MIT Quantum Information Science group. *Quantum Information Processing Seminar*.

2021-04-26, UT Austin quantum information center. *Group meeting*.

2021-04-23, AIDE-QC. *All hands meeting*.

2021-04-21, Quantum Systems Accelerator (QSA). *Science session*.

2021-02-01, Quantum Information Processing (QIP 2021).

2020-08-26, AIDE-QC. *Verification and debugging thrust meeting*.

2020-06-02, APS DAMOP 2020.

2019-05-30, APS DAMOP 2019.

2018-03-08, APS March Meeting 2018.

2017-06-07, APS DAMOP 2017.

Outreach and Equity

During graduate school, I was involved with the following organizations:

- **IGenSpectrum —** "Identity and Gender Spectrum." Student group for the LGBTQ+ community in Berkeley Physics. I served as an officer.
- **Respect is Part of Research —** Annual workshop aimed at improving department climate and preventing sexual violence and sexual harassment. I served each year as a facilitator, and helped to organize the workshop.
- **Bay Area Scientists in Schools —** Program in which local researchers teach science lessons to elementary school students around the Bay Area. I served as a teacher and a member of the Steering Committee.

Positionality and Languages

My ancestry is mostly German and Czech; “Kahanamoku” in my married name comes from my spouse, who is Hawaiian. I grew up in northern Vermont.

I speak English natively, and am conversational in Spanish and French (albeit with a Quebec accent!). My competency in Hawaiian is also gradually increasing. *Fun fact:* I contributed the Hawaiian language keyboard layout that is now included in most Linux distributions!