Bill Fefferman

Quantum Information and Computer Science (QuICS)
University of Maryland/National Institute of Standards and Technology
College Park, MD. 20742 **U.S.A.**

Phone: 630.673.1334
email: wjf@umd.edu
URL: http://www.umiacs.umd.edu/~wjf

Current positions

2014–present *Postdoctoral Scholar*, Quantum Information and Computer Science (QuICS), University of Maryland Institute for Advanced Computer Studies (UMIACS), University of Maryland

2015–present *Guest Researcher*, National Institute of Standards and Technology, Applied and Computational Mathematics Division

Areas of specialization

Theoretical Computer Science • Computational Complexity Theory • Quantum Computation and Cryptography

Brief Description of Research Interest

My research focuses on understanding the power of quantum computation. The goal is not only to understand the theoretical power of quantum computers of the indefinite future, but also to develop the foundations of computational complexity to rigorously analyze the capabilities and limitations of present-day and near-term quantum devices which are not yet fully scalable quantum computers. Furthermore, I am interested in using these capabilities and limitations to better understand the potential for cryptography in a fundamentally quantum mechanical world.

Education

2014 PH.D in Computer Science, California Institute of Technology, Pasadena, CA

- Advisors: Alexei Kitaev and Christopher Umans
- Committee: Venkat Chandrasekaran, Alexei Kitaev, John Preskill, Christopher Umans

2011 M.S in Computer Science, California Institute of Technology, Pasadena, CA
2008 B.S in Computer Science, The University of Chicago, Chicago, IL
2008 B.A in Mathematics, The University of Chicago, Chicago, IL

Previous Positions

2009-2011 *Graduate Research Fellow*
Institute for Quantum Information, California Institute of Technology. Pasadena, CA

2008 *Adjunct Research Staff member*
Quantum Information Group, NEC Laboratories. Princeton, NJ

2006,2007, 2014 *Adjunct Research Staff member*
Institute for Defense Analysis, Center for Communications Research. Princeton, NJ

Grants

2016 Co-authored a successful grant proposal from the Army Research Office

- Proposal title: "Complexity-theoretic foundations for near-term quantum computers"
- ARO Broad Agency Anouncement: W911NF-12-R-0012-04. Topic 6.2 (QIS)

Publications

- **The Power of Unentanglement** with S. Aaronson, S. Beigi, A. Drucker, P. Shor

  In Theory of Computing, 5(1):1-42, 2009.

  Also in Proceedings, Twenty-third IEEE Conference on Computational Complexity (CCC 2008), College Park, MD.

- **Pseudorandom Generators and the** BQP **vs** PH **Problem** with C. Umans

  Featured talk, Fourteenth Workshop on Quantum Information Processing (QIP 2011), Singapore.

- **On Quantum Computing and Pseudorandomness**

  M.S Thesis, California Institute of Technology, 2011.

- **On Beating the Hybrid Argument** with E. Viola, R. Shaltiel, C. Umans

  In Theory of Computing, 9(26):809-843, 2013

  Also in Proceedings, Third Conference on Innovations in Theoretical Computer Science (ITCS 2012), Cambridge, MA.

- **On the Power of Quantum Fourier Sampling**

  Ph.D Thesis, California Institute of Technology, 2014.

- **On the Power of Quantum Fourier Sampling** with C. Umans

  In Proceedings of the Eleventh Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016), Berlin, Germany.

- **Quantum vs Classical Proofs and Subset Verification** with S. Kimmel

  Submitted, 2015.

- **Quantum Merlin Arthur with Exponentially Small Gap** with C. Lin

  Submitted, 2016.

- **A Complete Characterization of Unitary Quantum Space** with C. Lin

  Accepted talk, Twentieth Workshop on Quantum Information Processing (QIP 2017), Seattle, Washington.

- **On Quantum Obfuscation** with G. Alagic.

  Accepted talk, Sixth International Conference on Quantum Cryptography (QCrypt 2016), Washington D.C.

- **Computational Security of Quantum Encryption** with G. Alagic, A. Broadbent, T. Gagliardoni, C. Schaffner, and M. St. Jules.

  Accepted talk, Sixth International Conference on Quantum Cryptography, (QCrypt 2016), Washington D.C.

  Also in Proceedings of Ninth International Conference on Information Theoretic Security (ICITS 2016), Tacoma, Washington, US.

- **Space-Efficient Error Reduction for Unitary Quantum Computations** with H. Kobayashi, C. Lin, T. Morimae, and H. Nishimura.

  In Proceedings of the Fourty-third International Colloquium on Automata, Languages, and Programming (ICALP 2016), Tacoma, Washington, US.

  Also Accepted talk, Sixteenth Asian Quantum Information Science Conference (AQIS 2016), Taipei, Taiwan.

- **Exact Sampling Hardness of Ising Spin Models** with A.V Gorshkov and M. Foss-Feig.

  Submitted, 2016.

- **Complexity of Sampling as an Order Parameter** with A. Deshpande, M. Foss-Feig, and A.V Gorshkov.

  Submitted, 2016.

Selected Invited and Contributed Talks

8.17.2016 • **Invited speaker**, Workshop on Semi-Quantum Computing, Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

4.15.2016 • **Invited speaker**, Heilbronn and QALGO Quantum Algorithms meeting, Cambridge University, Cambridge, UK

10.7.2016 • **Invited talk**, QMATH seminar, University of Copenhagen, Copenhagen, Denmark

10.4.2016 • **Invited talk**, Quantum Physics Seminar, Slovak Academy of Sciences, Bratislava, Slovakia

9.28.2016 • **Contributed talk**, Theory of Quantum Computation, Communication, and Cryptography Conference (TQC 2016), Berlin, Germany

9.15.2016 • **Contributed talk**, International Conference on Quantum Cryptography (QCrypt 2016), Washington D.C

8.30.2016 • **Invited talk**, Institute for Quantum Information Seminar, California Institute of Technology, Pasadena, California

7.12.2016 • **Contributed talk**, International Colloquium on Automata, Languages, and Programming (ICALP 2016), Rome, Italy

5.4.2016 • **Invited talk**, Quantum Computation Seminar, University of Technology Sydney, Sydney, Australia

7.15.2015 • **Invited talk**, Institute for Quantum Information Seminar, California Institute of Technology, Pasadena, California

5.20.2015 • **Invited talk**, Applied Math Seminar, National Security Agency, Fort Meade, Maryland

1.24.2014 • **Invited talk**, Algorithms and Complexity Seminar, Centrum Wiskunde & Informatica, Amsterdam, The Netherlands

1.10.2012 • **Contributed talk**, Innovations in Theoretical Computer Science (ITCS 2012), Massachusetts Institute of Technology, Cambridge, Massachusetts

5.17.2011 • **Invited talk**, James Franck Institute Seminar, Department of Physics, University of Chicago, Chicago, Illinois

5.30.2011 • **Invited talk**, Theory of Computation Seminar, University of Washington, Seattle, Washington

1.14.2011 • **Featured talk**, Workshop on Quantum Information Processing (QIP 2011), Singapore, Singapore

Service

8.1-8.5.2016 • *Chair*, QuICS Workshop on $\mathsf{QMA}(2)$ and the Complexity of Entanglement, University of Maryland, College Park, Maryland.

Organized an international workshop at QuICS on the computational power of quantum entanglement.

2009-present • *Referee*, Symposium on the Theory of Computing (STOC), Workshop on Quantum Information Processing (QIP), Theory of Quantum Computation, Communication, and Cryptography Conference (TQC), APPROX-RANDOM Conference, Physical

Review Letters, Quantum Information and Computation Journal, New Journal of Physics, Journal of Computer and System Sciences, Chicago Journal of Theoretical Computer Science