

Joseph Fitzsimons

Curriculum Vitae

Professional Career

- 2013–Present **Assistant Professor**, Singapore University of Technology and Design, Singapore.
- 2013–Present **Research Assistant Professor**, Centre for Quantum Technologies, Singapore.
- 2010–2013 **Senior Research Fellow**, Centre for Quantum Technologies, Singapore.
- 2007–2010 **Senior Research Fellow**, Department of Materials, University of Oxford, UK.
- 2007–2010 **Junior Research Fellow**, Merton College, Oxford, UK.
- 2006–2007 **College Lecturer (GTA)**, Oriel College, Oxford, UK.

Education

- 2005–2007 **Doctorate (DPhil)**, Department of Materials, University of Oxford, UK.
- 2000–2004 **Bachelor of Science (BSc) in Theoretical Physics**, *First Class Honours*, University College Dublin, Ireland.

Doctoral Thesis

- Title *Architectures for Quantum Computation under Restricted Control*
- Supervisors Dr Simon Benjamin & Dr Dan Browne

Awards and Distinctions

- 2016 **Innovators Under 35 Asia Honouree**, MIT Technology Review.
- 2013 **NRF Fellowship**, National Research Foundation, Singapore.
- 2007 **Master of Arts (MA) by resolution**, University of Oxford, UK.
- 2005–2007 **Helmore Award**, Oxford University Society, UK.
- 2005–2007 **DTA Scholarship**, Engineering and Physical Sciences Research Council, UK.
- 2006 **Waterson Scholarship**, St. Anne's College, Oxford, UK.
- 2006 **Travel Scholarship**, Worshipful Company of Founders, UK.
- 2004–2005 **Government of Ireland Scholar**, Irish Research Council for Science, Engineering and Technology, Ireland.

Research Grants

- 2015–2018 **Principal Investigator**, *Quantum primitives for secure computing*, Grant No. FA2386-15-1-4082, Asian Office of Aerospace Research and Development, Air Force Office of Scientific Research, USA. Total value US\$449,047.
- 2013–2018 **Principal Investigator**, *Methods for verifying quantum computation*, Grant No. NRF-NRFF2013-01, National Research Foundation, Singapore. Total value S\$3,519,000.
- 2013–2016 **Principal Investigator**, *Start-up Research Grant*, SRG-EPD-2013-066, Singapore University of Technology and Design, Singapore. Total value S\$100,000.

2008 **Principal Investigator**, *Fault-tolerant quantum memories in densely packed systems*, Nuffield Foundation, UK. Total value £1,400.

Teaching Experience

- 2013–Present **Singapore University of Technology and Design**.
Undergraduate: 10.004 Advanced Math II: Linear algebra and multivariable calculus.
Graduate: 30.510 Quantum Computation and Quantum Information.
Mentoring: Academic mentor to 10 undergraduate students. Cohort Mentor to cohort F08.
- 2009–2010 **Merton College**.
Undergraduate: Mathematical Methods, Research Talks course.
- 2006–2007 **Oriel College**.
Undergraduate: Mechanics, Special Relativity, Optics, Circuit Theory, Electromagnetism, Condensed Matter and Condensed Matter Physics Devices courses.
- 2005–2006 **St. Anne's College**.
Undergraduate: Thermodynamics revision lectures, Statistical Mechanics.

Visiting Positions

- 2011 **Visiting Lecturer**, Department of Physics, University College Dublin, Ireland.
- 2007–2008 **Visiting Research Associate/Postdoctoral Research Fellow**, Institute for Quantum Computing, University of Waterloo, Canada.
- 2006 **Exchange Fellow**, Macquarie University, Australia.

Research Supervision

- Undergraduate 4 current undergraduate research student, 2 previous interns.
Graduate 4 current PhD students (all have passed QE), 1 successfully graduated.
Postdocs 4 current postdoctoral researchers and 3 former.

Professional Memberships

American Physical Society (APS), Association for Computing Machinery (ACM) and Association Computability in Europe (CiE).

Reviewing Activity

- Journals Nature Communications, Physical Review Letters, Physical Review X, Physical Review A, Physics Letters A, Scientific Reports, Proceedings of the Royal Society A, Philosophical Transactions of the Royal Society A, Quantum Information and Computation, International Journal of Quantum Information, Mathematical Structures in Computer Science, ACM Journal on Emerging Technologies in Computing Systems.
- Conferences FOCS, STOC, QIP, IFIP SEC, AQIS, TQC, CiE, DCM and various workshops.
- Textbooks University of Chicago Press, Elsevier.
- Grants Air Force Office of Scientific Research (USA), Unity Through Knowledge Fund (Croatia), Rutherford Discovery Fellowship (New Zealand).

Committee Activity

Conference committees

- 2016 **Programme Committee**, Theory of Quantum Computation Computation, Communication and Cryptography (TQC).
- 2010 **Programme Committee**, Developments in Computational Models (DCM).
- 2009 **Programme Committee**, Logical Aspects of Fault-Tolerance (LAFT).
- 2009 **Assistant Organizer**, Quantum Correlations and Computations (QuCoCo).
- 2007 **Local Organizing Committee**, Measurement-Based Quantum Computation (MBQC).

Academic committees

- 2013–present **Board of Graduate Studies**, SUTD.
- 2015–present **EPD Development Committee**, SUTD.
- 2013–2015 **EPD Budget Committee**, SUTD.
- 2013–2015 **EPD Distinguished Lecture Series Committee**, SUTD.
- 2007-2010 **Governing Body**, Merton College.
- 2007-2010 **Materials Department Faculty**, University of Oxford.
- 2007-2010 **Congregation**, University of Oxford.

Other committees

- 2016 **Judging Panel**, Singapore International Mathematical Challenge.
- 2013 **Judging Panel**, Singapore Mentoring Programme.
- 2012 **Judging Panel**, Singapore International Mathematical Challenge.

Recent Invited Talks

- 2015 **Second Workshop on Secure Computing**, University of Tokyo, Japan.
- 2015 **Quantum Computational Complexity**, ICALP workshop, Kyoto, Japan.
- 2015 **Workshop for Quantum Repeaters and Networks (Panel discussant)**, Asilomar, USA.
- 2015 **Trustworthy Quantum Information**, University of Michigan, USA.
- 2015 **Advances in Quantum Cryptography**, Institut Henri Poincaré, France.
- 2015 **First Workshop on Secure Computing**, University of Tokyo, Japan.
- 2015 **QIP (Plenary talk)**, University of Technology Sydney, Australia.
Note: I was unable to present at QIP due to a scheduling conflict with ITCS at which the work was being published. The talk was instead given by my co-author Thomas Vidick.
- 2014 **Australia-Japan Workshop on Multi-user Quantum Networks**, UTS, Sydney, Australia.
- 2014 **Coherent Control of Complex Quantum Systems**, OIST, Okinawa, Japan.
- 2014 **Quantum Games and Protocols**, UC Berkeley, Berkeley, USA.

Publications

- 2016 Liming Zhao, Carlos A Pérez-Delgado, and Joseph F Fitzsimons, Fast graph operations in quantum computation, *Physical Review A*, 93:032314.
Scott Aaronson, Adam Bouland, Joseph Fitzsimons, and Mitchell Lee. The space “just above” BQP. In *Proceedings of the 2016 Conference on Innovations in Theoretical Computer Science*. ACM, 2016.
- 2015 Zhikuan Zhao, Jack K Fitzsimons, and Joseph F Fitzsimons, Quantum assisted gaussian process regression, *arXiv preprint arXiv:1512.03929*.
Peter P Rohde, Keith R Motes, Paul A Knott, Joseph Fitzsimons, William J Munro, and Jonathan P Dowling, Evidence for the conjecture that sampling generalized cat states with linear optics is hard, *Physical Review A*, 91(1):012342.
Carlos A Pérez-Delgado and Joseph F Fitzsimons, Iterated gate teleportation and blind quantum computation, *Physical Review Letters*, 114(22):220502.
Yingkai Ouyang, Si-Hui Tan, and Joseph Fitzsimons, Quantum homomorphic encryption from quantum codes, *arXiv preprint arXiv:1508.00938*.
Yingkai Ouyang and Joseph F Fitzsimons, Permutation-invariant codes encoding more than one qubit, *arXiv preprint arXiv:1512.02469*.
Michal Hajdušek, Carlos A Pérez-Delgado, and Joseph F Fitzsimons, Device-independent verifiable blind quantum computation, *arXiv preprint arXiv:1502.02563*.
Joseph F Fitzsimons and Michal Hajdušek, Post hoc verification of quantum computation, *arXiv preprint arXiv:1512.04375*.
Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local hamiltonian problem. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, pages 103–112. ACM, 2015.
Joseph Fitzsimons, Jonathan Jones, and Vlatko Vedral, Quantum correlations which imply causation, *Scientific Reports*, 5(18281).
- 2014 Li Yu, Carlos A Pérez-Delgado, and Joseph F Fitzsimons, Limitations on information-theoretically-secure quantum homomorphic encryption, *Physical Review A*, 90(5):050303.
Si-Hui Tan, Joshua A Kettlewell, Yingkai Ouyang, Lin Chen, and Joseph F Fitzsimons, A quantum approach to fully homomorphic encryption, *arXiv preprint arXiv:1411.5254*.
Naomi H Nickerson, Joseph F Fitzsimons, and Simon C Benjamin, Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links, *Physical Review X*, 4(4):041041.
Tomoyuki Morimae, Keisuke Fujii, and Joseph F Fitzsimons, On the hardness of classically simulating the one clean qubit model, *Physical Review Letters*, 112(13):130502.
Vedran Dunjko, Joseph F Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. In *Advances in Cryptology–ASIACRYPT 2014*, pages 406–425. Springer Berlin Heidelberg, 2014.
- 2013 Peter P Rohde, Joseph F. Fitzsimons, and Alexei Gilchrist, Information capacity of a single photon, *Physical Review A*, 88(2):022310.
Atul Mantri, Carlos A Pérez-Delgado, and Joseph F Fitzsimons, Optimal blind quantum computation, *Physical Review Letters*, 111(23):230502.
Joseph F. Fitzsimons, Eleanor G Rieffel, and Valerio Scarani. The quantum frontier. In J. Zander and P.J. Mosterman, editors, *Computation for Humanity: Information Technology to Advance Society*. CRC Press, 2013.

- Stefanie Barz, Joseph F. Fitzsimons, Elham Kashefi, and Philip Walther, Experimental verification of quantum computation, *Nature Physics*, 9(11):727–731.
- 2012 Peter P Rohde, Joseph F. Fitzsimons, and Alexei Gilchrist, Quantum walks with encrypted data, *Physical Review Letters*, 109(15):150501.
- Joseph F. Fitzsimons and Elham Kashefi, Unconditionally verifiable blind computation, *arXiv preprint arXiv:1203.5217*.
- Joseph Fitzsimons and Elham Kashefi, Universal blind quantum computation, *Bulletin of the American Physical Society*, 57.
- Joseph Fitzsimons, Quantum changes in the cryptographic landscape, *Hakin9 Extra*, (14):26–30.
- Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F. Fitzsimons, Anton Zeilinger, and Philip Walther, Demonstration of blind quantum computing, *Science*, 335(6066):303–308.
- 2011 Yuichiro Matsuzaki, Simon C Benjamin, and Joseph Fitzsimons, Magnetic field sensing beyond the standard quantum limit under the effect of decoherence, *Physical Review A*, 84(1):012103.
- Yuichiro Matsuzaki, Simon C Benjamin, and Joseph Fitzsimons, Entangling unstable optically active matter qubits, *Physical Review A*, 83(6):060303.
- Joseph Fitzsimons, Review of algebraic cryptanalysis by gregory v. bard, *ACM SIGACT News*, 42(2):14–18.
- Tom Close, Femi Fadugba, Simon C Benjamin, Joseph Fitzsimons, and Brendon W Lovett, Rapid and robust spin state amplification, *Physical Review Letters*, 106(16):167204.
- JD Biamonte, V Bergholm, James D Whitfield, J Fitzsimons, and Alan Aspuru-Guzik, Adiabatic quantum simulators, *AIP Advances*, 1(2):022126.
- 2010 Marcus Schaffry, Erik M Gauger, John JL Morton, Joseph Fitzsimons, Simon C Benjamin, and Brendon W Lovett, Quantum metrology with molecular ensembles, *Physical Review A*, 82(4):042114.
- Yuichiro Matsuzaki, Simon C Benjamin, and Joseph Fitzsimons, Probabilistic growth of large entangled states with low error accumulation, *Physical Review Letters*, 104(5):050501.
- Yuichiro Matsuzaki, Simon C Benjamin, and Joseph Fitzsimons, Distributed quantum computation with arbitrarily poor photon detection, *Physical Review A*, 82(1):010302.
- Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Measurement-based and universal blind quantum computation. In *Formal Methods for Quantitative Aspects of Programming Languages*, pages 43–86. Springer Berlin Heidelberg, 2010.
- 2009 Jonathan A Jones, Steven D Karlen, Joseph Fitzsimons, Arzhang Ardavan, Simon C Benjamin, G Andrew D Briggs, and John JL Morton, Magnetic field sensing beyond the standard quantum limit using 10-spin noon states, *Science*, 324(5931):1166–1168.
- Joseph Fitzsimons and Jason Twamley, Quantum fault tolerance in systems with restricted control, *Electronic Notes in Theoretical Computer Science*, 258(2):35–49.
- Earl T Campbell and Joseph Fitzsimons, An introduction to one-way quantum computing in distributed architectures, *International Journal of Quantum Information*, 8(1-2):219.
- Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science – FOCS '09*, pages 517–526. IEEE, 2009.
- Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp. Anonymous quantum communication. In *Information Theoretic Security*, pages 181–182. Springer Berlin Heidelberg, 2009.

- 2007 Joseph Francis Fitzsimons. *Architectures for quantum computation under restricted control*. PhD thesis, University of Oxford, 2007.
- Joseph Fitzsimons, Li Xiao, Simon C Benjamin, and Jonathan A Jones, Quantum information processing with delocalized qubits under global control, *Physical Review Letters*, 99(3):30501.
- Joseph Fitzsimons and Jason Twamley, Globally controlled fault tolerant quantum computation, *arXiv preprint arXiv:0707.1119*.
- Earl T Campbell, Joseph Fitzsimons, Simon C Benjamin, and Pieter Kok, Efficient growth of complex graph states via imperfect path erasure, *New Journal of Physics*, 9(6):196.
- Earl T Campbell, Joseph Fitzsimons, Simon C Benjamin, and Pieter Kok, Adaptive strategies for graph-state growth in the presence of monitored errors, *Physical Review A*, 75(4):042303.
- Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs, and Alain Tapp. Anonymous quantum communication. In *Advances in Cryptology – ASIACRYPT 2007*, pages 460–473. Springer Berlin Heidelberg, 2007.
- 2006 Joseph Fitzsimons and Jason Twamley, Globally controlled quantum wires for perfect qubit transport, mirroring, and computing, *Physical Review Letters*, 97(9):090502.
- Simon C Benjamin, Daniel E Browne, Joe Fitzsimons, and John JL Morton, Brokered graph-state quantum computation, *New Journal of Physics*, 8(8):141.
- 2005 J Fitzsimons and J Twamley, Superballistic diffusion of entanglement in disordered spin chains, *Physical Review A*, 72(5):050301.