Vlad Gheorghiu – Curriculum Vitae

Phone: +1-(519) 741-7185
Email: vgheorgh@gmail.com
Office: IQC-QNC 3112
Web page: http://vsoftco.github.io
Citizenship: Canadian, European Union (Romania)

Institute for Quantum Computing
at the University of Waterloo
200 University Drive W
Waterloo, ON N2L-3G1, Canada

Education and Work Experience

- 2017 – currently, CEO, President and Co-Founder of **softwareQ Inc.**, Waterloo ON, Canada.
- 2016 – currently, quantum risk researcher, **evolutionQ Inc.**, Waterloo ON, Canada.
- 2013 – currently, Postdoctoral Researcher, **Institute for Quantum Computing at the University of Waterloo**, Waterloo ON, Canada. Involved in the CryptoWorks21 Quantum-Safe Cryptographic Infrastructure Program. Member of the European Telecommunications Standards Institute (ETSI) Quantum-Safe Cryptography Standardization Group.
- 2011 – 2013, Postdoctoral Researcher, **Institute for Quantum Information Science**, Faculty member, **Department of Mathematics and Statistics, University of Calgary**, Calgary AB, Canada.
- 2010 – 2011, Postdoctoral Research Associate, **Carnegie Mellon University**, Pittsburgh, PA 15213, USA, working with Prof. Robert B. Griffiths.
- 2004 – 2010, PhD in Physics, Quantum Information Theory, **Carnegie Mellon University**, Pittsburgh, PA 15213, USA. Dissertation Title: "Separable Operations, Graph Codes and the Location of Quantum Information". Thesis advisor: Prof. Robert B. Griffiths.
- 1999 – 2003, B.S. in Theoretical Physics, **University of Bucharest**, Romania. Graduated with a GPA of 9.81 on a scale from 1 to 10. Diploma Thesis Title: "Adiabatic Perturbation Theory in Quantum Mechanics". Thesis advisor: Prof. Gheorghe Nenciu.

Honors and Awards

- 2011–2013, $40,000 (CAD) Pacific Institute for the Mathematical Sciences Postdoctoral Fellowship Award under the Collaborative Research Group in Mathematics of Quantum Information. Application success rate $\sim 15\%$.
- 2012 Postdoctoral Fellow Departmental Competition, Department of Mathematics and Statistics, University of Calgary, Canada. 3 nominations out of 10 candidates.
- 2004–2010, University Tuition Scholarship, Carnegie Mellon University, USA.
- 1994, 1997, 1998, Romanian National Physics Olympiad Laureate.

Publications

2019

- Beatrice Nash, *Vlad Gheorghiu* and Michele Mosca, **"Quantum circuit optimizations for NISQ architectures**", arXiv:1904.01972 [quant-ph] (2019)

- *Vlad Gheorghiu* and Michele Mosca, **"Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes**", arXiv:1902.02332 [quant-ph] (2019)
- Olivia Di Matteo, *Vlad Gheorghiu* and Michele Mosca, **Fault tolerant resource estimation of quantum random-access memories**, arXiv:1902.01329 [quant-ph] (2019)

2018

- *Vlad Gheorghiu* and Michele Mosca, **A resource estimation framework for quantum attacks against cryptographic functions, part 4**, Global Risk Institute, Toronto, Canada, quantum risk assessment report Feb. 2018 - Aug. 2018 (2018).
- *Vlad Gheorghiu* and Michele Mosca, **A resource estimation framework for quantum attacks against cryptographic functions, part 3**, Global Risk Institute, Toronto, Canada, quantum risk assessment report Sep. 2017 - Feb. 2018 (2018).

2017

- *Vlad Gheorghiu*, Sergey Gorbunov, Michele Mosca and Bill Munson, **Quantum-Proofing the Blockchain**, white paper for The Blockchain Research Institute, Toronto, Canada (2017).
- *Vlad Gheorghiu* and Michele Mosca, **A resource estimation framework for quantum attacks against cryptographic functions, part 2**, Global Risk Institute, Toronto, Canada, quantum risk assessment report Feb. 2017 - Aug. 2017 (2017).
- *Vlad Gheorghiu* and Michele Mosca, **A resource estimation framework for quantum attacks against cryptographic functions, part 1**, Global Risk Institute, Toronto, Canada, quantum risk assessment report Sep. 2016 - Feb. 2017 (2017).
- Jacob Marks, Tomas Jochym-O'Connor and *Vlad Gheorghiu*, **Comparison of fault-tolerant thresholds for planar qudit geometries**, arXiv:1701.02335 [quant-ph] (2017), New Journal of Physics **19**, 113022 (2017).

2016

- Matthew Amy, Olivia Di Matteo, *Vlad Gheorghiu*, Michele Mosca, Alex Parent and John Schanck, **"Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3**", in the proceedings of **Selected Areas in Cryptography (SAC) 2016, Newfoundland, Canada**, Lecture Notes in Computer Science, vol 10532, pp. 317-337, Springer, Cham. Cryptology ePrint Archive: Report 2016/992, arXiv:1603.09383 [quant-ph] (2016). Accepted as a hot-topic contribution to **PQCrypto 2016**, Fukoaka, Japan, invited talk at the **Quantum Computer Science Workshop**, April 17-22, 2016, Banff, Canada.

2015

- *Vlad Gheorghiu* and Barry C. Sanders, **"Nonzero Classical Discord**", arXiv:1407.5507 [quant-ph], Physical Review Letters **115**, 030403 (2015).
- Srinivasan Arunachalam, *Vlad Gheorghiu*, Tomas Jochym-O'Connor, Michele Mosca and Priyaa Varshinee Srinivasan, **"On the Robustness of Bucket Brigade Quantum RAM**", arXiv:1502.03450 [quant-ph] (2015), New Journal of Physics **17**, 123010 (2015), contributed talk in the proceedings of the **TQC 2015**, Bruxelles, Belgium, contributed talk **AQIS 2015**, Seoul, South Korea

2014

- *Vlad Gheorghiu*, **"Quantum++ - A C++11 Quantum Computing Library"**, arXiv:1412.4704 [quant-ph] (2014), contributed talk at the **Quantum Programming and Circuits Workshop**, June 8-11, 2015, IQC, University of Waterloo, Canada, invited talk at the **BIRS Quantum Computer Science Workshop**, April 17-22, 2016, Banff, Canada.
- *Vlad Gheorghiu*, **"Standard Form of Qudit Stabilizer Groups"**, arXiv:1101.1519 [quant-ph], Physics Letters A **378**, 505–509 (2014).
- German Luna, Samuel Reid, Bianca de Sanctis and *Vlad Gheorghiu*, **"A Combinatorial Approach to Quantum Error Correcting Codes"**, arXiv:1304.6743 [math], Discrete Mathematics, Algorithms and Applications, vol. **6**, 1450054 (2014).

2013

- *Vlad Gheorghiu* and Barry C. Sanders, **"Accessing Quantum Secrets via Local Operations and Classical Communication"**, arXiv:1305.0805 [quant-ph], Physical Review A **88**, 022340 (2013).
- Shmuel Friedland, *Vlad Gheorghiu* and Gilad Gour, **"Universal Uncertainty Relations"**, arXiv:1304.6351 [quant-ph], Physical Review Letters **111**, 230401 (2013).

2012

- Patrick J. Coles, *Vlad Gheorghiu* and Robert B. Griffiths, **"Consistent Histories for Tunneling Molecules Subject to Collisional Decoherence"**, arXiv:1205.6188 [quant-ph] (2012), Physical Review A **86**, 042111 (2012).
- *Vlad Gheorghiu* and Gilad Gour, **"Multipartite Entanglement Evolution Under Separable Operations"**, arXiv:1205.2667 [quant-ph] (2012), Physical Review A **86**, 050302 (Rapid Communications) (2012).
- *Vlad Gheorghiu*, **"Generalized Semiquantum Secret-Sharing Schems"**, arXiv:1204.1072 [quant-ph], Physical Review A **85**, 052309 (2012).

2011

- Patrick J. Coles, Li Yu, *Vlad Gheorghiu* and Robert B. Griffiths, **"Information Theoretic Treatment of Tripartite Systems and Quantum Channels"**, arXiv:1006.4859 [quant-ph], Physical Review A **83**, 062338 (2011).

2010

- *Vlad Gheorghiu*, **"Separable Operations, Graph Codes and the Location of Quantum Information"**, Carnegie Mellon University PhD thesis, arXiv:1006.4888 [quant-ph], also available at ProQuest Dissertation & Theses under Publication No. AAT 3470169, ISBN 9781124122816 (2010).
- *Vlad Gheorghiu*, Li Yu and Scott M. Cohen, **"Local Cloning of Entangled States"**, Physical Review A **82**, 022313 (2010).
- *Vlad Gheorghiu* and Shiang Yong Looi, **"Construction of Equally Entangled Bases in Arbitrary Dimensions via Quadratic Gauss Sums and Graph States"**, Physical Review A **81**, 062341 (2010).
- *Vlad Gheorghiu*, Shiang Yong Looi and Robert B. Griffiths, **"Location of Quantum Information in Additive Graph Codes"**, Physical Review A **81**, 032326 (2010).

2008

- *Vlad Gheorghiu* and Robert B. Griffiths, **"Separable Operations on Pure States"**, Physical Review A **78**, 020304 (Rapid Communications) (2008).
- Shiang Yong Looi, Li Yu, *Vlad Gheorghiu* and Robert B. Griffiths, **"Quantum Error Correcting Codes Using Qudit Graph States"**, Physical Review A **78**, 042303 (2008).

2007

- *Vlad Gheorghiu* and Robert B. Griffiths, **"Entanglement Transformations Using Separable Operations"**, Physical Review A **76**, 032310 (2007).

Conferences/Workshops/Summer Schools/Talks

- Invited speaker, **Quantum for Business**, Mountain View, CA USA , 12 December 2018: Vlad Gheorghiu, "Quantum threat: What matters today?".
- Invited speaker, **Data Science and Quantum Computing Workshop**, Triumf, Vancouver, Canada, 27 June 2018: Vlad Gheorghiu, "IQC - Univ. of Waterloo, Quantum Computing Efforts Quantum computing in the near to medium-term range".
- Invited speaker, **Vietnam Blockchain Week**, Ho Chi Minh City, Vietnam 8 March 2018: Vlad Gheorghiu, "Quantum-resistant cryptography and its impact on Blockchains".
- Invited speaker, **SecTor**, Toronto, Canada, 15 November 2017: Michele Mosca and Vlad Gheorghiu, "The quantum threat: what really matters today?"
- Invited speaker, **Creative Destruction Lab**, Toronto, Canada, 22 September 2017: Vlad Gheorghiu, "Surface codes: an introduction".
- Invited speaker, **ETSI/IQC Quantum Safe Workshop**, London, UK, 15 September 2017: Vlad Gheorghiu, "Resource Estimation for Quantum Cryptanalysis".
- Invited speaker, **Creative Destruction Lab**, Toronto, Canada, 6 September 2017: Vlad Gheorghiu, "Quantum++ A modern C++ quantum computing simulator".
- Invited speaker, **Turing Inc. Workshop**, Mayacamas Ranch, Calistoga CA, USA, 24 August 2017: Vlad Gheorghiu, "Quantum Resource Estimation".
- Invited keynote speaker, **Internet Economy Summit**, Hong Kong, 10 April 2017: Vlad Gheorghiu, "Quantum Computing in the Age of Big Data".
- Invited talk, **Quantum Computer Science Workshop**, Banff AB, Canada, 21 April 2016: Vlad Gheorghiu, "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3".
- Invited talk, **Quantum Computer Science Workshop**, Banff AB, Canada, 19 April 2016: Vlad Gheorghiu, "Software demo: Quantum++".
- Contributed talk, **Quantum Programming and Circuits Workshop**, Waterloo ON, Canada, 9 June 2015: Vlad Gheorghiu, "Quantum++ – A modern C++ quantum computing library".
- Invited talk, **North South Dialogue in Mathematics**, Edmonton AB, Canada, 4 May 2012: Vlad Gheorghiu, "Quantum entanglement: properties and evolution".
- Contributed talk, **Southwest Quantum Information and Technology (SQUINT 2012), 14th Annual Meeting**, Albuquerque NM, USA, 16-19 February 2012: Vlad Gheorghiu, "Optimal hybrid quantum secret sharing schemes via stabilizer codes and twirling of symplectic structures".

- Contributed poster, **Conceptual Foundations and Foils for Quantum Information Processing**, Perimeter Institute, Canada, 9-13 May 2011: Vlad Gheorghiu, “Information-theoretical study of collisional decoherence of chiral molecules in a gas".
- Invited talk, **University of Bristol**, Bristol, UK, 13 January 2010: Vlad Gheorghiu, “Location of Quantum Information in Additive Graph Codes", hosted by Prof. Richard Jozsa.
- Invited talk, **Max-Plank-Institut für Quantenoptik**, Garching, Germany, 12 January 2010: Vlad Gheorghiu, “Location of Quantum Information in Additive Graph Codes", hosted by Prof. Ignacio Cirac.
- Poster presentation, **The Thirteen Workshop on Quantum Information Processing (QIP 2010)**, 18-22 January 2010, Zürich, Switzerland: Vlad Gheorghiu, Scott M. Cohen and Robert B. Griffiths, “Most Entangled States Cannot be Locally Cloned".
- Poster presentation, **The Twelfth Workshop on Quantum Information Processing (QIP 2009)**, 12-16 January 2009, Santa Fe NM, USA: Vlad Gheorghiu, Shiang Yong Looi and Robert B. Griifiths, “Location of Quantum Information in Additive Quantum Codes".
- Poster presentation, **3-rd International Conference on Quantum Information (ICQI 2008)**, 13-16 July 2008, Boston MA, USA: Vlad Gheorghiu and Robert B. Griffiths, “Separable Operations on Pure States".
- Participant, **2-nd International Conference on Quantum Information (ICQI 2007)**, 13-15 June, 2007, Rochester NY, USA.
- Presented around 50 seminars/talks at the **CMU Quantum Information Seminar**, during 2005 – 2011. Titles/summaries/talks available at http://quantum.phys.cmu.edu/QIP/index.html.

Teaching Experience

- Fall 2012, Instructor for Calculus I (MATH 251) in the Mathematics and Statistics Department at the University of Calgary. Students enrolled: 121. Duties: course preparation, homework preparation, exam preparation and grading. Student evaluations overall score 5.88/7, detailed report available on request.
- Summer 2012, Instructional Skills Workshop teaching certificate, available on request.
- Fall 2011, Instructor for Calculus I (MATH 251) in the Mathematics and Statistics Department at the University of Calgary. Students enrolled: 118. Duties: course preparation, homework preparation, exam preparation and grading. Student evaluations overall score 5.22/7, detailed report available on request.
- Spring 2011, Supervised PhD student Ananth Tenneti. Duties: meeting the student weekly and guide him on his research track.
- Spring 2009, Supervised PhD student Chang-You Lin. Duties: taught the student introductory quantum information theory and get him started on a research project, that finally became a refereed published paper, Physical Review A **81**, 032326 (2010).
- Spring 2008, Spring 2010, homework grading and guest lecturer for Quantum Information and Computation Theory Course (PHYS 33-658) taught by my PhD advisor Robert B. Griffiths.
- Fall 2004, Spring 2005, Fall 2005, Spring 2006, Carnegie Mellon University, Teaching Assistant for Physics for Engineering Students I (PHYS 33-106). Duties: lab/recitation material preparation, homework and exam grading.

Research Interests

The following areas in Quantum Information

- Quantum software, quantum architectures.
- Fault tolerance
- Quantum resource estimation for cryptographic algorithms.
- Classical-quantum separation, correlation measures.
- Uncertainty relations.
- LOCC, separable operations and the role of entanglement as a physical resource.
- Graph states and graph codes, applications to quantum error correction.
- Additivity problems for quantum channel capacity.
- Location of quantum information in multipartite quantum systems, relations between quantum channels and their complement.

Professional Activity

Referee for:

- Nature
- Physical Review Letters
- Physical Review A
- New Journal of Physics
- Quantum Information Processing
- Quantum Information and Computation
- Quantum Science and Technology
- Physics Letters A
- International Journal of Quantum Information
- International Journal of Theoretical Physics
- Entropy
- Optics Communications
- IEEE Security & Privacy

Computer Skills

- C++ (expert knowledge)
- C, Java, MATLAB, Mathematica (extensive knowledge).
- UNIX/Linux, Windows (extensive knowledge).
- Ruby, Python, HTML, Perl, PHP (fair knowledge).

Foreign Languages

- English: Excellent reading/writing/speaking.
- French: Good reading/writing, fair speaking.
- Romanian (native language).

Other Interests

- Computer Science, C++ programming, Mathematics, Quantitative Finance, Guitar playing, Reading, Hiking, Pool (8 ball), Soccer, Tennis.

References (research)

- **Prof. Michele Mosca**, Institute for Quantum Computing
  University of Waterloo, Canada
  Email: mmosca@uwaterloo.ca
  Phone: +1-(519) 888-4567 ext. 37484

- **Prof. Robert B. Griffiths**, Carnegie Mellon University, USA
  Email: rgrif@andrew.cmu.edu
  Phone: +1-(412) 268-2765

- **Prof. Barry C. Sanders**, IQST and University of Calgary, Canada
  Email: sandersb@ucalgary.ca
  Phone: +1-(403) 220-3939

- **Prof. Gilad Gour**, IQST and University of Calgary, Canada
  Email: gour@ucalgary.ca
  Phone: +1-(403) 220-3939

- **Prof. Scott M. Cohen**, Duquesne University, USA
  Email: cohensm@duq.edu
  Phone: +1-(412) 396-6353

- **Prof. Edward Gerjuoy**, University of Pittsburgh, USA
  Email: gerjuoy@pitt.edu
  Phone: +1-(412) 624-9025

References (teaching)

- **Prof. Claude Laflamme**, University of Calgary, Canada
  Email: laf@math.ucalgary.ca
  Phone: +1-(403) 220-3962

- **Prof. Robert B. Griffiths**, Carnegie Mellon University, USA
  Email: rgrif@andrew.cmu.edu
  Phone: +1-(412) 268-2765

- **Prof. Helmut Vogel, USA**, Carnegie Mellon University
  Email: vogel@heps.phys.cmu.edu
  Phone: +1-(412) 268-2757

- **Prof. James Russ, USA**, Carnegie Mellon University
  Email: russ@heps.phys.cmu.edu
  Phone: +1-(412) 268-2755