IQC - Univ. of Waterloo Quantum Computing Efforts

Quantum computing in the near to medium-term range

Dr. Vlad Gheorghiu [1,2,3]

[1] Institute for Quantum Computing, University of Waterloo, Canada

[2] softwareQ Inc, Waterloo, Canada

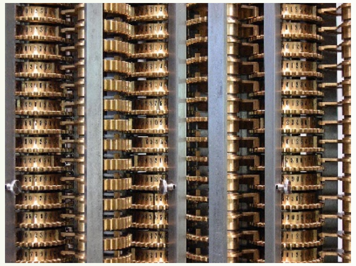
[3] evolutionQ Inc, Waterloo, Canada

vlad@softwareq.ca

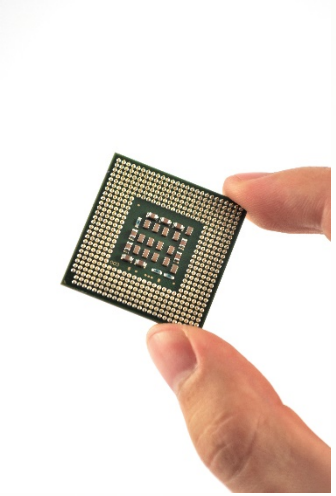
vlad.gheorghiu@uwaterloo.ca

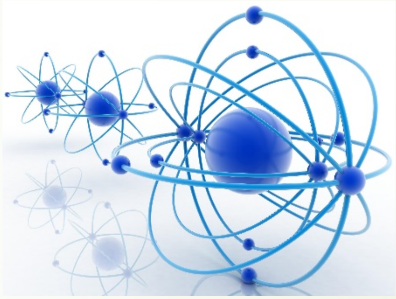
TRIUMF 2018, Vancouver, Canada

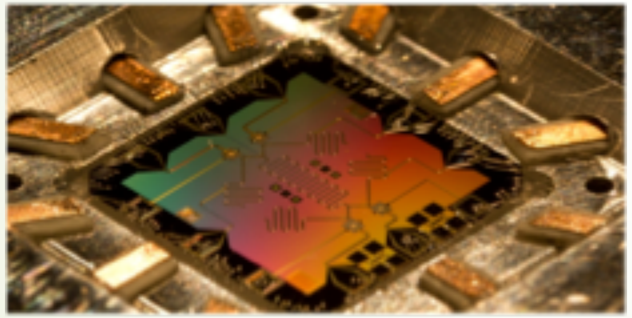
A new paradigm for information and computation: *quantum computation*



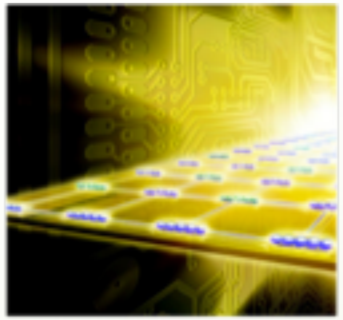
By Carsten Ullrich



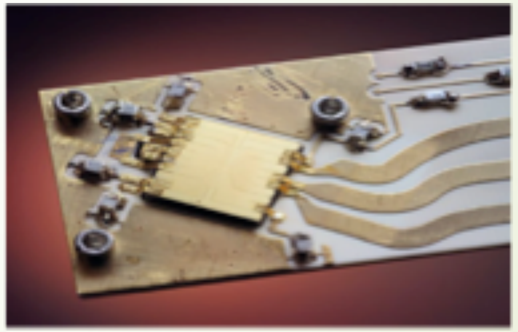




E. Lucero, D. Mariantoni, and M. Mariantoni



© Harald Ritsch



Y. Colombe/NIST

Both a blessing and a curse

Powerful new quantum technologies are emerging, which promise tremendous benefits…

…but also pose serious threats to our communications, control and information security.

Where are we today?

REVIEW SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret[1,2] and R. J. Schoelkopf[1*]

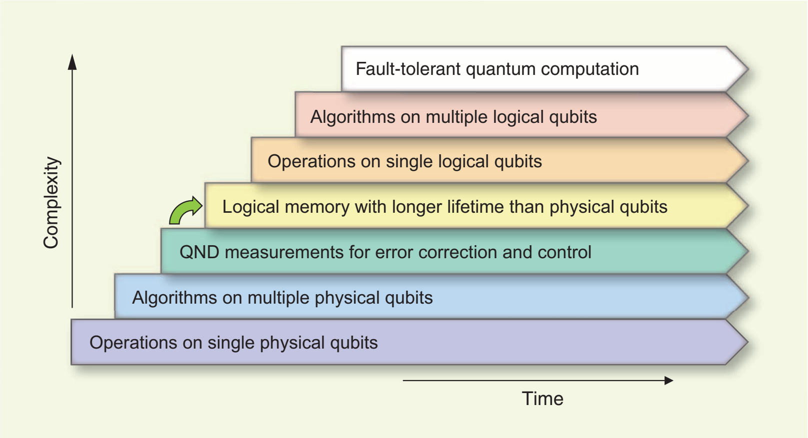


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

POPULAR SCIENCE
WANT MORE?

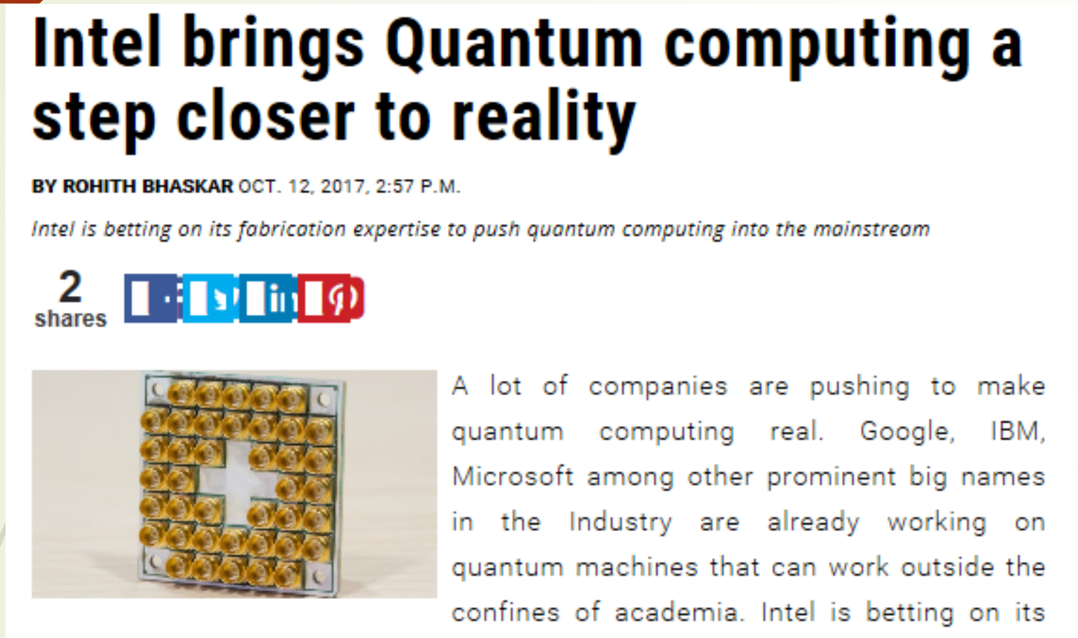
China is opening a new quantum research supercenter

The country wants to build a quantum computer with a million times the computing power presently in the world.

By Jeffrey Lin and P.W. Singer *October 10, 2017*

Lithium's Big

NATIONAL LABORATORY FOR QUANTUM INFORMATION SCIENCES
The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.



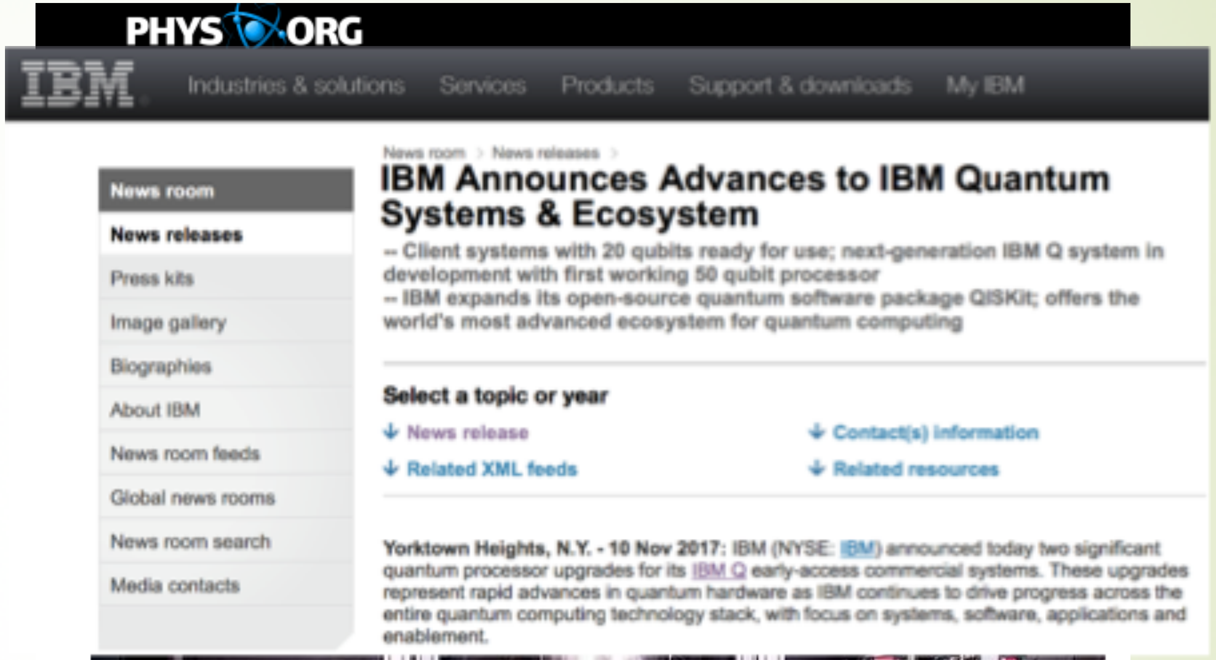
Intel brings Quantum computing a step closer to reality

BY ROHITH BHASKAR OCT. 12, 2017, 2:57 P.M.

Intel is betting on its fabrication expertise to push quantum computing into the mainstream

2 shares

A lot of companies are pushing to make quantum computing real. Google, IBM, Microsoft among other prominent big names in the Industry are already working on quantum machines that can work outside the confines of academia. Intel is betting on its



PHYS ORG

IBM Industries & solutions Services Products Support & downloads My IBM

News room > News releases >

News room
News releases
Press kits
Image gallery
Biographies
About IBM
News room feeds
Global news rooms
News room search
Media contacts

IBM Announces Advances to IBM Quantum Systems & Ecosystem

-- Client systems with 20 qubits ready for use; next-generation IBM Q system in development with first working 50 qubit processor

-- IBM expands its open-source quantum software package QISKit; offers the world's most advanced ecosystem for quantum computing

Select a topic or year

News release
Contact(s) information
Related XML feeds
Related resources

Yorktown Heights, N.Y. - 10 Nov 2017: IBM (NYSE: IBM) announced today two significant quantum processor upgrades for its IBM Q early-access commercial systems. These upgrades represent rapid advances in quantum hardware as IBM continues to drive progress across the entire quantum computing technology stack, with focus on systems, software, applications and enablement.

NISQ Era

arXiv.org > quant-ph > arXiv:1801.00862

Search or Article

(Help | Advanced sear

Quantum Physics

Quantum Computing in the NISQ era and beyond

John Preskill

(Submitted on 2 Jan 2018 (v1), last revised 27 Jan 2018 (this version, v2))

Noisy Intermediate-Scale Quantum (NISQ) technology will be available in the near future. Quantum computers with 50-100 qubits may be able to perform tasks which surpass the capabilities of today's classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably. NISQ devices will be useful tools for exploring many-body quantum physics, and may have other useful applications, but the 100-qubit quantum computer will not change the world right away --- we should regard it as a significant step toward the more powerful quantum technologies of the future. Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing.

Comments: 22 pages. Based on a Keynote Address at Quantum Computing for Business, 5 December 2017. (v2) Minor corrections
Subjects: **Quantum Physics (quant-ph)**; Strongly Correlated Electrons (cond-mat.str-el)
Cite as: arXiv:1801.00862 **[quant-ph]**
(or arXiv:1801.00862v2 **[quant-ph]** for this version)

Submission history

From: John Preskill [view email]
[v1] Tue, 2 Jan 2018 23:43:08 GMT (23kb)
[v2] Sat, 27 Jan 2018 23:46:40 GMT (23kb)

Types of quantum computers and what can we do with them

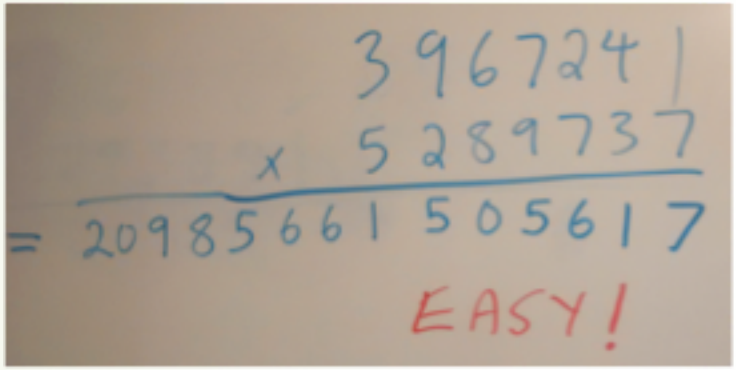
- Fault tolerant (universal quantum computers)
  - Still a long way to go…
  - IBM, Google, Microsoft, Rigetti
  - Proof-of-concept quantum computing
  - Quantum "supremacy" tests?!
  - Can we break crypto with them? NOT YET.
  - Can we do "cool things"? Most likely!
- Quantum annealers (noisy qubits)
  - DWave
  - Useful now, optimization, quantum machine learning

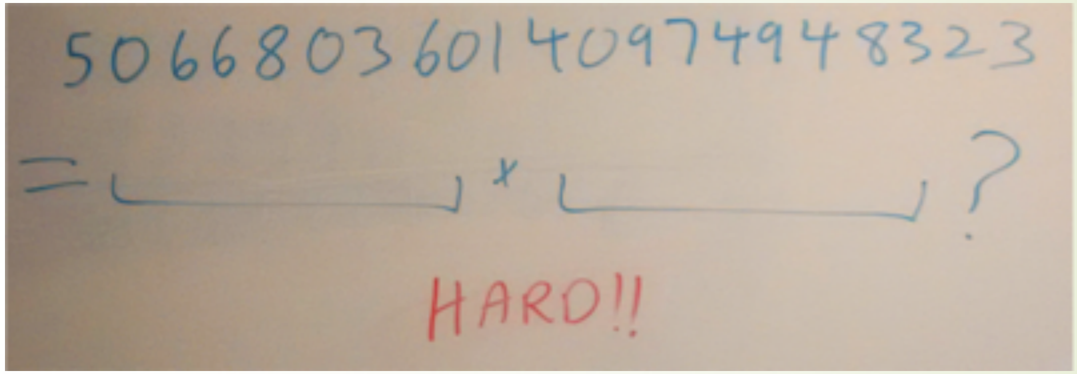
What are quantum computers good for?

- "Global patterns": seeing the "forest" without observing the "trees"
- Example: The sequence 34, 12, 54, 38, 57, 34, 12, 54, 38, 57, 34, 12, … has a period of length 5
- Imagine a sequence with an astronomically large period.
- With a handful of quantum glimpses: "length of period = 729672482463". Based on Quantum Phase Estimation and Quantum Fourier Transform.
- "any specific value in the sequence = ???"

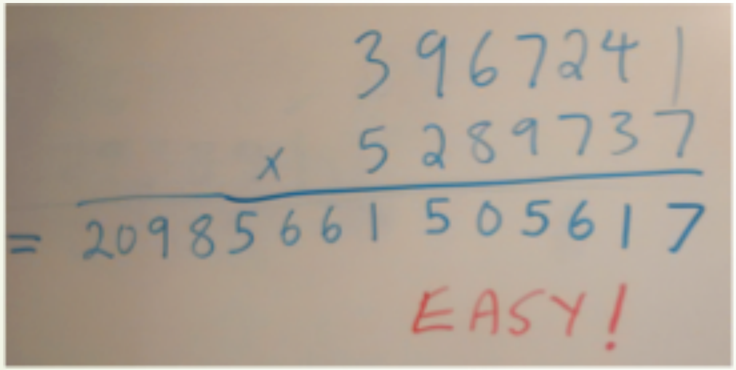
Shor's algorithm for factoring (1994)

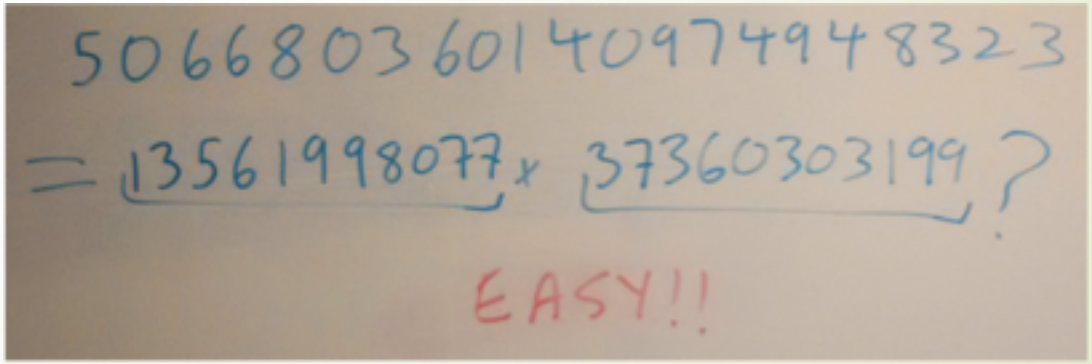
- Exponentially faster than any "classical" algorithm
- Classically:





- On a quantum computer:





Shor's algorithm for factoring (1994)

Peter Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal on Computing **26**, 1484 (1997)

Running time: $O((\log N)^2 \log\log(N)$log log log(N)), i.e. poly(log(N)).

Best classical algorithm (number sieve): $e^{O(\sqrt{\log N \log\log N})}$.

Best heuristic: $e^{O((\log N \log\log N)^{1/3})}$.

Exponential improvement, based on **Quantum Fourier Transform.**

Variant of it can be used to break the discrete-log problem

Grover's algorithm for searching (1997)

- Searching through "unordered" data
- Quadratically faster – $O(\sqrt{N})$ vs $O(N)$
- 1'000'000 books – only 1'000 "queries"!

Grover's algorithm for searching (1997)

Lov Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack", Phys. Rev. Lett. **79**, 325 (1997)

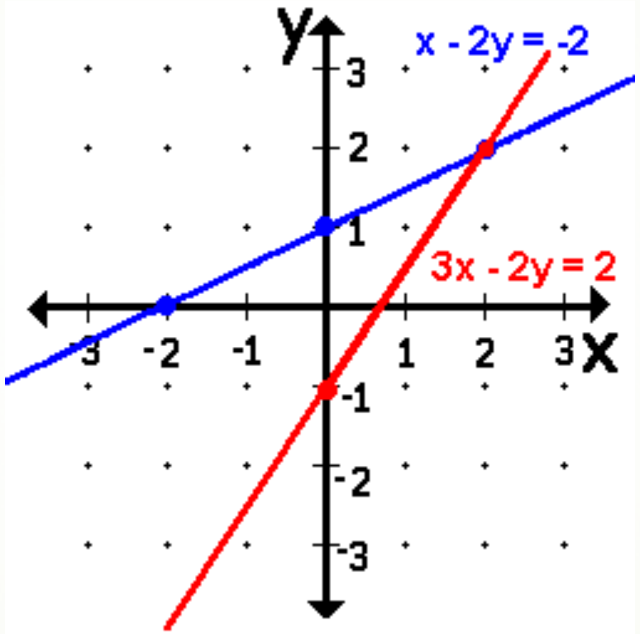
Running time: $O(\sqrt{N})$ vs $O(N)$

Quadratic improvement, based on **Amplitude Amplification**

Proposed uses: Quantum Cryptanalysis, Quantum Machine Learning

Solving systems of linear equations (2009)

A. Harrow, A. Hassidim and S. Lloyd, " Quantum Algorithm for Linear Systems of Equations", Phys. Rev. Lett. **103**, 150502 (2009)



- **Exponentially faster** than any classical algorithm, applications in quantum machine learning
- Other algorithms: Deutsch-Jozsa, Simon's etc.
- Stephen Jordan's (NIST) http://math.nist.gov/quantum/zoo/

What's the catch?

- Quantum computing is **fragile**
- Need redundancy (error-correction)

- There is a way: **Quantum Error Correction (P. Shor again)** – thousands of **physical** qubits for 1 good logical qubit -> millions of **physical** qubits circuit blowup.
- Experimentally, this is a **REALLY HARD PROBLEM**! We are getting there, closer to the threshold!
- Mostly an engineering problem. Engineers **always** manage do it (somehow)!

IQC at University of Waterloo

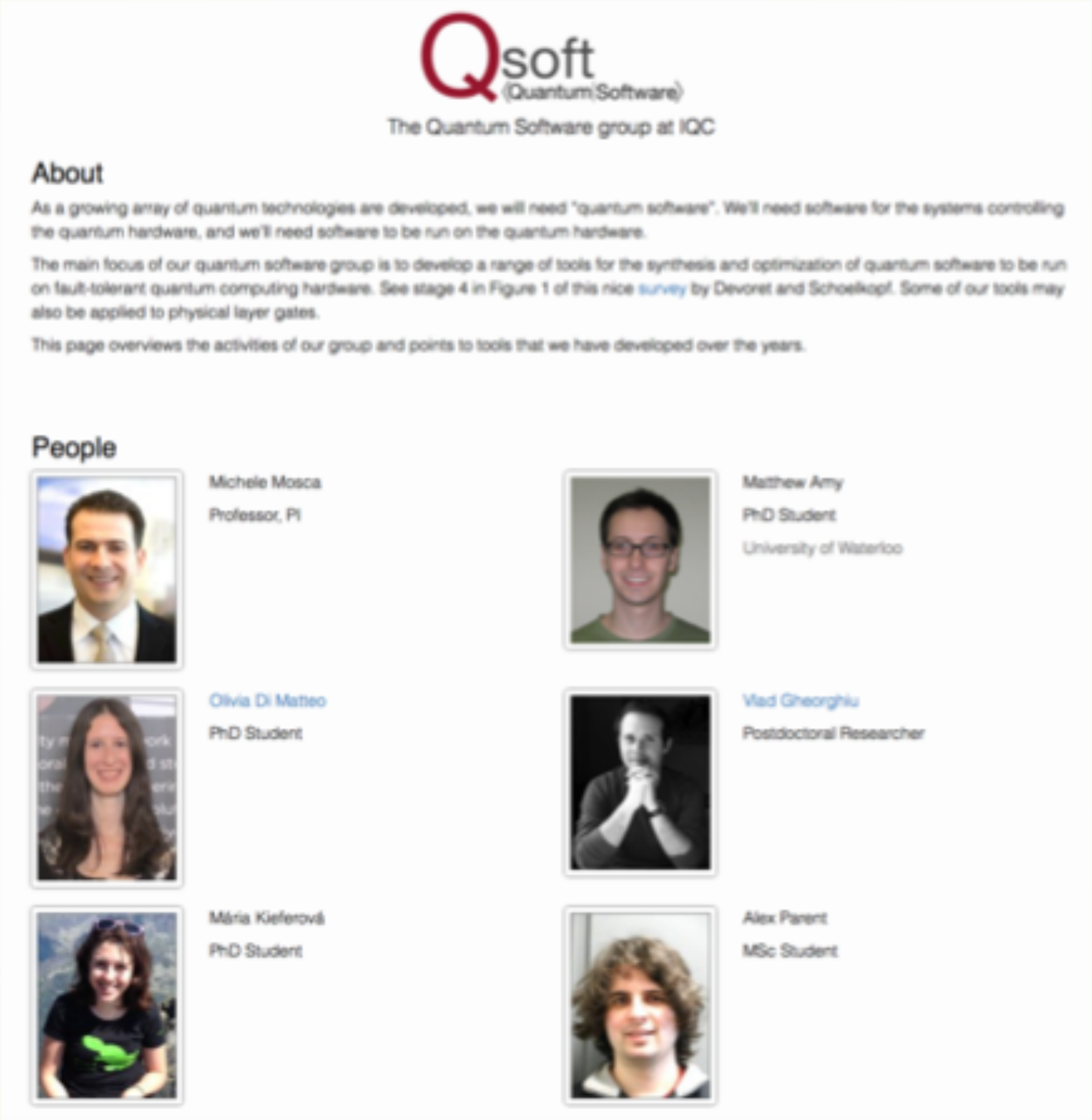
https://uwaterloo.ca/institute-for-quantum-computing/

Areas of research

- Quantum Error Correction and Fault Tolerance
- Quantum Complexity Theory
- Quantum Algorithms
- Quantum Information Theory
- Quantum Software
- Quantum Cryptography
- Spin-based Quantum Information Processing
- Nanoelectronics-based Quantum Information Processing
- Optical Quantum Information Processing

Areas of research

- Quantum Error Correction and Fault Tolerance
- Quantum Complexity Theory
- Quantum Algorithms
- Quantum Information Theory
- **Quantum Software**
- **(Post)-Quantum Cryptography**
- **Quantum Machine Learning**
- Spin-based Quantum Information Processing
- Nanoelectronics-based Quantum Information Processing
- Optical Quantum Information Processing
- Etc.



Qsoft (Quantum|Software)

The Quantum Software group at IQC

About

As a growing array of quantum technologies are developed, we will need "quantum software". We'll need software for the systems controlling the quantum hardware, and we'll need software to be run on the quantum hardware.

The main focus of our quantum software group is to develop a range of tools for the synthesis and optimization of quantum software to be run on fault-tolerant quantum computing hardware. See stage 4 in Figure 1 of this nice survey by Devoret and Schoelkopf. Some of our tools may also be applied to physical layer gates.

This page overviews the activities of our group and points to tools that we have developed over the years.

People

Michele Mosca
Professor, PI

Matthew Amy
PhD Student
University of Waterloo

Olivia Di Matteo
PhD Student

Vlad Gheorghiu
Postdoctoral Researcher

Mária Kieferová
PhD Student

Alex Parent
MSc Student

Research

Comparison of fault-tolerant thresholds for planar qudit geometries
Jacob Marks, Tomas J.-O'Connor and Vlad Gheorghiu
New Journal of Physics **19**, 113022 (2017).
https://doi.org/10.1088/1367-2630/aa939a

Technology mapping of reversible circuits to Clifford+T quantum circuits
N. Abdessaied, M. Amy, M. Soeken, R. Drechsler
https://infoscience.epfl.ch/record/216835

Complexity of reversible circuits and their quantum implementations
N. Abdessaied, M. Amy, R. Drechsler, M. Soeken
http://www.sciencedirect.com/science/article/pii/S0304397516000220

Parallelizing quantum circuit synthesis
O. Di Matteo, M. Mosca
Quantum Science and Technology **1** (1) (2016)
http://iopscience.iop.org/article/10.1088/2058-9565/1/1/015003/meta

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3
M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck
https://arxiv.org/abs/1603.09383

Verified compilation of space-efficient reversible circuits
M. Amy, M. Roetteler, K. Svore
http://arxiv.org/abs/1603.01635

≡ All Research

Software

https://github.com/QCT-IQC

Quantum++

Download

Version 1.0 - Release Candidate 4, 24 January 2018

Quantum++ is a modern C++11 general purpose quantum computing library, composed solely of template header files. Quantum++ is written in standard C++11 and has very low external dependencies, using only the Eigen 3 linear algebra header-only template library and, if available, the OpenMP multi-processing library.

Quantum++ is not restricted to qubit systems or specific quantum information processing tasks, being capable of simulating arbitrary quantum processes. The main design factors taken in consideration were the ease of use, high portability, and high performance. The library's simulation capabilities are only restricted by the amount of available physical memory. On a typical machine (Intel i5 8Gb RAM) Quantum++ can successfully simulate the evolution of 25 qubits in a pure state or of 12 qubits in a mixed state reasonably fast.

pQCS

Download

Version 1.2.0 - 27 May 2016

pQCS, short for "parallel quantum circuit synthesis", is a tool which leverages parallel collision finding algorithms to exactly synthesize multi-qubit circuits with optimal T-count. The details of the algorithm can be found in Olivia Di Matteo's MSc thesis.

pQCS is written in C++11, and comes in two 'flavours'. The first uses OpenMP for parallelization (making it suitable for use on a multi-core personal computer), and the second uses Boost.MPI (for use on clusters). pQCS has been tested extensively on Linux and Mac OS X. New features are actively under development.

Institute for Quantum Computing »

Norbert Lütkenhaus

Faculty, Professor

- Email: lutkenhaus.office@uwaterloo.ca
- Office: QNC 4129
- Office Phone: 519-888-4567 ext. 32870
- http://lutkenhausgroup.wordpress.com/
- Admin Support: Michele Roche

- **Unstructured QKD**
  Most QKD protocols that we analyze today have a high symmetry in signals and measurements. Key rate calculations are basically multi-parameter optimization with a non-linear objective function. The symmetry of QKD protocols allows us often to perform this optimization analytically. However, imperfections in experimental realizations often break the symmetry: Think for example at beam-splitters that do not have exact 50/50 splitting ratios, detectors that differ in their detection efficiency. Many protocols also have too many parameters, even if some symmetry persists. This often includes protocol implementations with side-channels (see below).Our group develops methods that allow to calculate canonically secret key rates for arbitrary QKD protocols. This method is based on the theory of convex optimization and allows for efficient numerical evaluations.
  Recent Publications:
  - *Unstructured quantum key distribution*
    Patrick J. Coles, Eric M. Metodiev, Norbert Lütkenhaus
    Nature Communications 7, 11712 (2016)

QKD Security Analysis Software

Our group has been developing numerical tools for analyzing QKD protocols. We developed a software package that allows to analyze simple finite-dimensional QKD protocols, which we make available here.

Download for Mac
Download for Windows

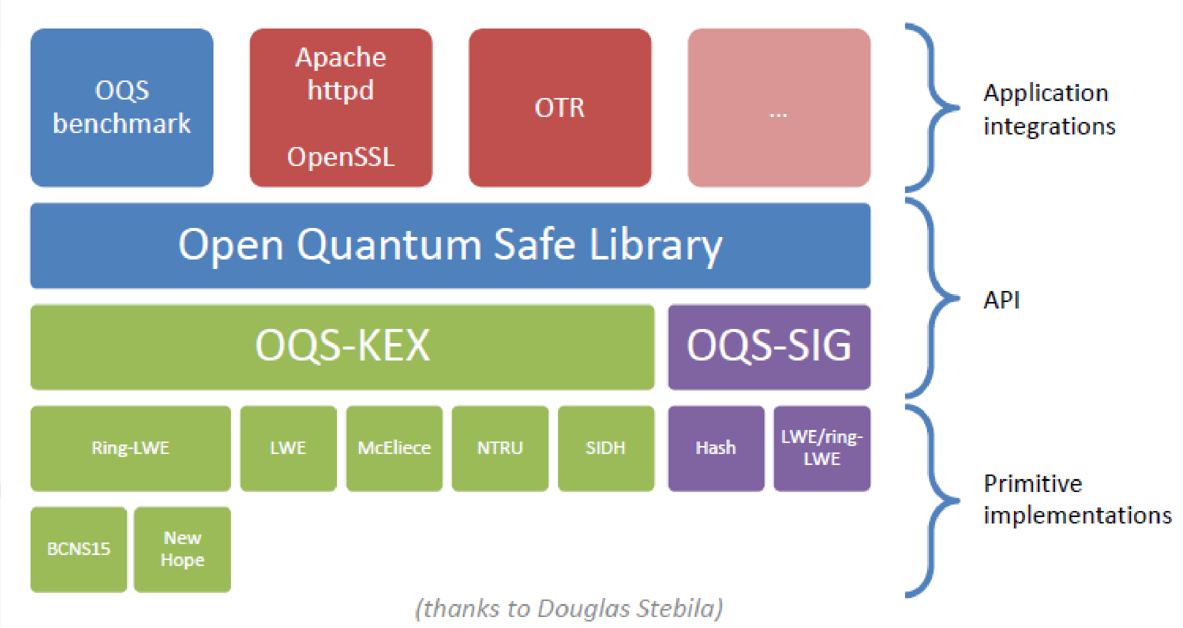
This package is a stand-alone applications. It has been written in Matlab, but does not require Matlab to run. Download the file and run the installer. A basic documentation is also available

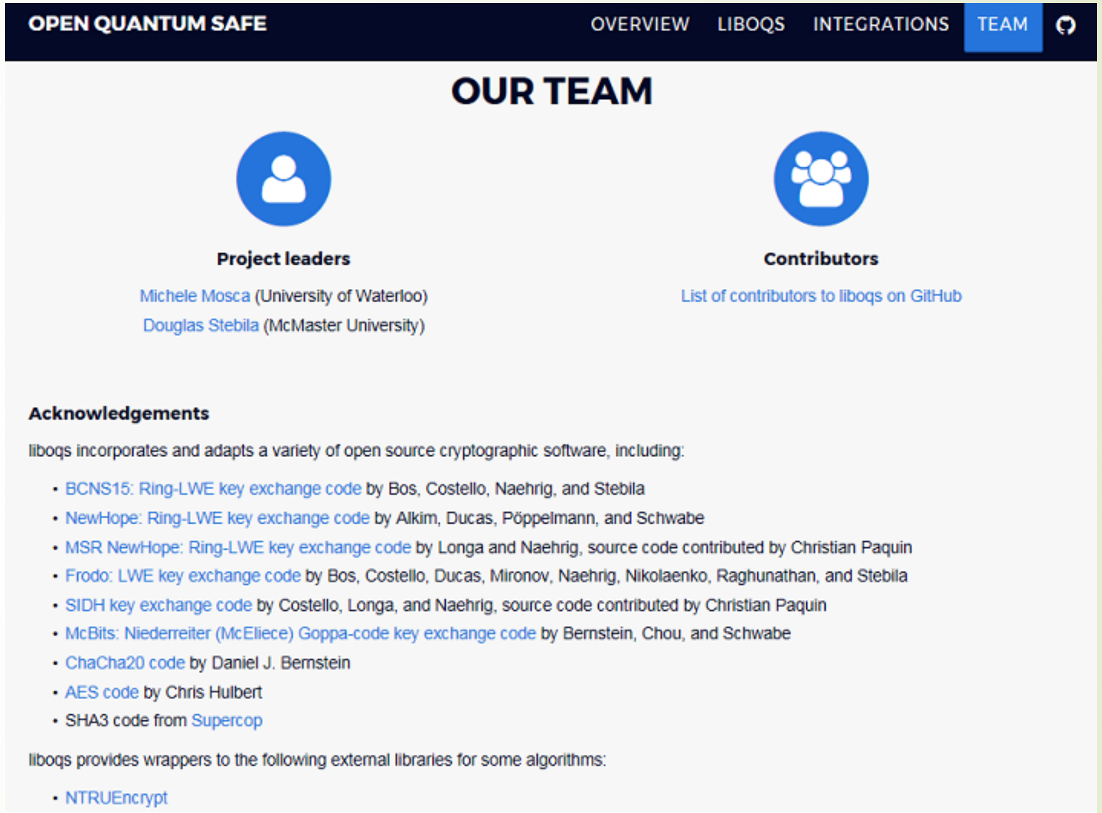
Download Manual

The simulation software is based on our publication

P.J. Coles, E. M. Metodiev, N. Lütkenhaus, "Numerical Approach for Unstructured Quantum key Distribution" Nature Communications, **7,11712**, (2016)


OPEN QUANTUM SAFE
OVERVIEW
LIBOQS
INTEGRATIONS
TEAM
openquantumsafe.org
OPEN QUANTUM SAFE
software for prototyping
quantum-resistant cryptography





OPEN QUANTUM SAFE OVERVIEW LIBOQS INTEGRATIONS TEAM

OUR TEAM

Project leaders

Michele Mosca (University of Waterloo)
Douglas Stebila (McMaster University)

Contributors

List of contributors to liboqs on GitHub

Acknowledgements

liboqs incorporates and adapts a variety of open source cryptographic software, including:

- BCNS15: Ring-LWE key exchange code by Bos, Costello, Naehrig, and Stebila
- NewHope: Ring-LWE key exchange code by Alkim, Ducas, Pöppelmann, and Schwabe
- MSR NewHope: Ring-LWE key exchange code by Longa and Naehrig, source code contributed by Christian Paquin
- Frodo: LWE key exchange code by Bos, Costello, Ducas, Mironov, Naehrig, Nikolaenko, Raghunathan, and Stebila
- SIDH key exchange code by Costello, Longa, and Naehrig, source code contributed by Christian Paquin
- McBits: Niederreiter (McEliece) Goppa-code key exchange code by Bernstein, Chou, and Schwabe
- ChaCha20 code by Daniel J. Bernstein
- AES code by Chris Hulbert
- SHA3 code from Supercop

liboqs provides wrappers to the following external libraries for some algorithms:

- NTRUEncrypt

Institute for Quantum Computing » Events » 2018 » May »

Quantum Machine Learning Symposium

TUESDAY, MAY 8, 2018 — 9:30 AM EDT

The Creative Destruction Lab (CDL) is hosting a half-day symposium to discuss recent advances in Quantum Machine Learning, its near-term industry applications, and opportunities for commercialization with private financing as a technology startup. Held at IQC, the symposium will include technical lectures by leading Quantum Machine Learning (QML) researchers Peter Wittek and Guillaume Verdon, an explanation of the CDL and its quantum program, as well as presentations by CDL alumni quantum ventures Xanadu, OTI Lumionics, and ProteinQure. Lunch is included.

Date: Tuesday, May 8
Time: 9:30am to 1:00pm
Location: Lazaridis Centre, QNC 1501

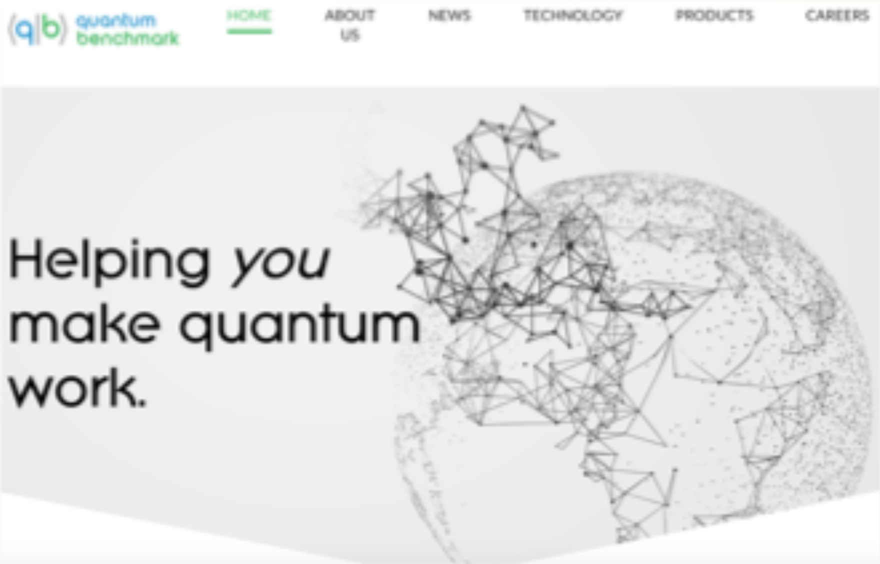
Training programs

Educational programs

We run several educational programs for students ranging from high school to graduate studies:

- Quantum Cryptography School for Young Students (QCSYS)
- Undergraduate School on Experimental Quantum Information Processing (USEQIP)
- Undergraduate Research Award (URA)
- Exchange programs
- Quantum Key Distribution (QKD) Summer School
- Quantum Innovators
- Schrödinger's Class

Spin-offs (non-exhaustive)



Take home

- Quantum computing is a disruptive technology, with a plethora of applications ranging from cyber-security to optimization and machine learning
- Need to act NOW
- Need to have a strong Canadian leadership in the area
- Need to educate industry players about quantum computing
  - Sort through the "hype"
  - Understand current and future benefits
  - Quantum "roadmaps"
- Need to train and hire adequate workforce
- Need more research for the NISQ regime
- Quantum software opportunities (similar to the "classical" software revolution that started in the 60s and it's still going on)

Thank you

Comments, questions and feedback are very welcome.

Vlad Gheorghiu

Co-Founder and CEO softwareQ Inc.
www.softwareq.ca

Post-doctoral fellow,
Institute for Quantum Computing, University of Waterloo

Quantum Risk Researcher
evolutionQ Inc. www.evolutionq.com

vlad@softwareq.ca
vlad.gheorghiu@uwaterloo.ca