Quantum Computing Update

Presentation to X9 working group

23 January 2020

Michele Mosca

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

softwareQ

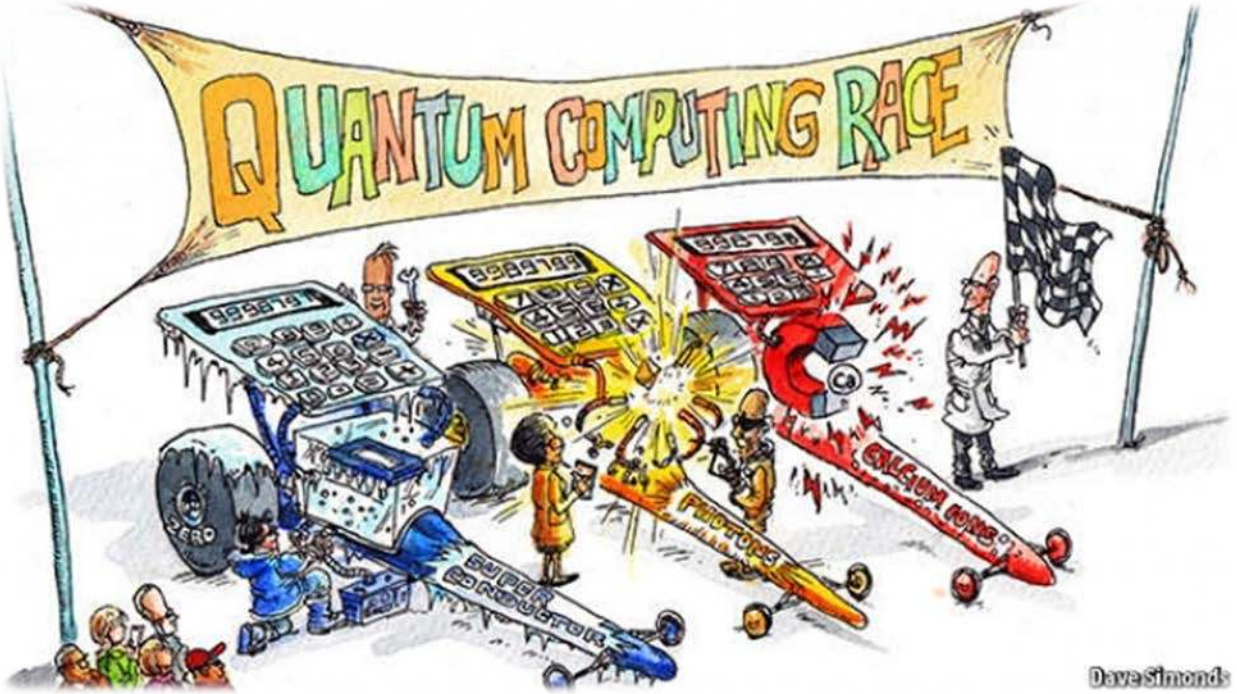
Quantum-Safe CANADA

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

QUANTUM INDUSTRY CANADA

evolution

CYBER SECURITY INSTITUTE AND PRIVACY UNIVERSITY OF WATERLOO



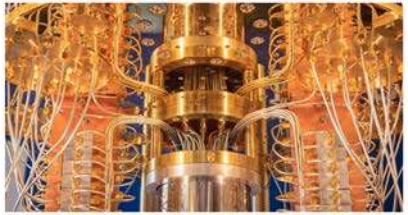
The Economist

COMPUTERS

IBM's new 53-qubit quantum computer is its biggest yet

The system will go online in October.

BY STEPHEN SHANKLAND | SEPTEMBER 18, 2019 5:00 AM PDT



A close-up view of the IBM Q quantum computer. The processor is in the silver-colored cylinder.
Stephen Shankland/CNET

30,223 views | Jan 8, 2020, 02:13pm

Forbes

IBM Doubles Its Quantum Computing Power Again

Rigetti Eyes Scaling with 128-Qubit Architecture
By George Leopold

August 10, 2018

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018

QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.

physicsworld

POLICY AND FUNDING | NEWS

Quantum Circuits bags $18m in first-round financing

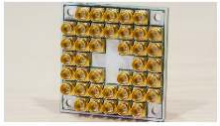
20 Nov 2017 Hamish Johnston

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

Search Bloomberg Sign In

Technology

Microsoft Edges Closer to Quantum Computer Based on Elusive Particle

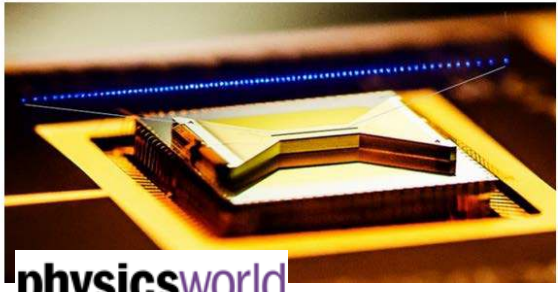
Researchers make Majorana fermions, but now must try to control them

By Jeremy Kahn
March 28, 2018, 11:48 AM EDT *Corrected March 28, 2018, 2:09 PM EDT*

QUANTUM NEWS

Ion-based commercial quantum computer is a first

17 Dec 2018



physicsworld

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

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.

Lithium's Big

Alibaba puts 11-qubits quantum power on public cloud

Together with Chinese Academy of Sciences, Alibaba Cloud has unleashed superconducting quantum computing services on its public cloud, running on a processor with 11 quantum bits of power.

By Eileen Yu for By The Way | March 1, 2018 -- 14:11 GMT (06:11 PST) | Topic: Cloud

South China Morning Post EDITION: INTERNATIONAL

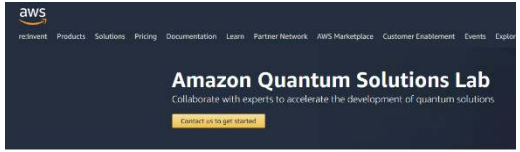
SCIENCE & RESEARCH

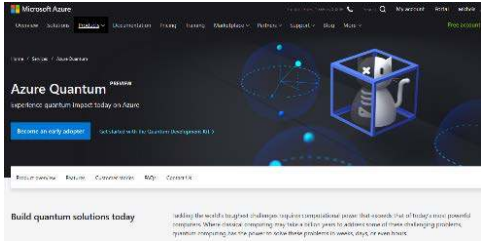
China's race for the mother of all supercomputers just got more crowded

Baidu, Alibaba and Tencent jockey for position in the development of quantum computing, which delivers a faster and more efficient approach to processing information than today's fastest computers

PUBLISHED : Monday, 12 March, 2018, 9:03am
UPDATED : Monday, 12 March, 2018, 9:02am

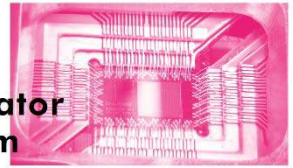
Baidu has entered the race to build quantum computers





CREATIVE DESTRUCTION LAB

CDL QML Incubator Stream



China's Alibaba Hires Quantum Computer Scientist Mario Szegedy

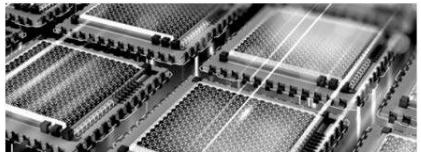
Tencent Quantum Laboratory is under construction, the next three major laboratories will provide a wealth of AI scenarios

"SNG is putting a lot of effort into the layout of artificial intelligence. At present, SNG has excellent labs, audio and video labs, and quantum labs. "Tang Dao-cheng, senior executive vice president of Tencent Group and president of the Social Networking Group (SNG), said in his opening speech.

THE WALL STREET JOURNAL.

IBM's Quantum-Computing Service Tops 100 Customers

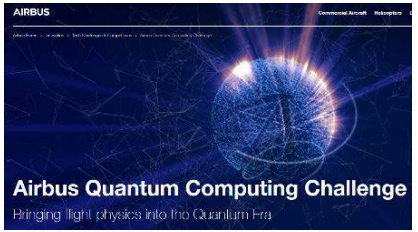
INTEL'S QUANTUM EFFORTS TIED TO NEXT-GEN MATERIALS APPLICATIONS



D-Wave

D-Wave's Ocean Software

Ocean software is a suite of tools **D-Wave Systems** provides on the **D-Wave GitHub repository** for solving hard problems with quantum computers.



softwareQ

DESIGNING QUANTUM SOFTWARE

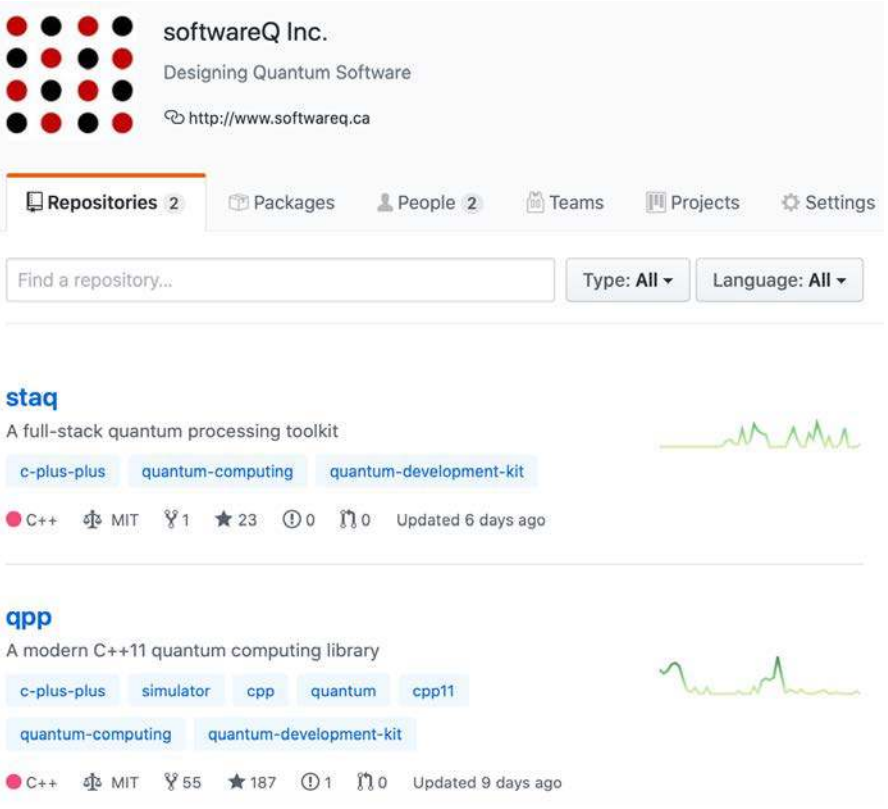
Quantum++: A modern C++ quantum computing library

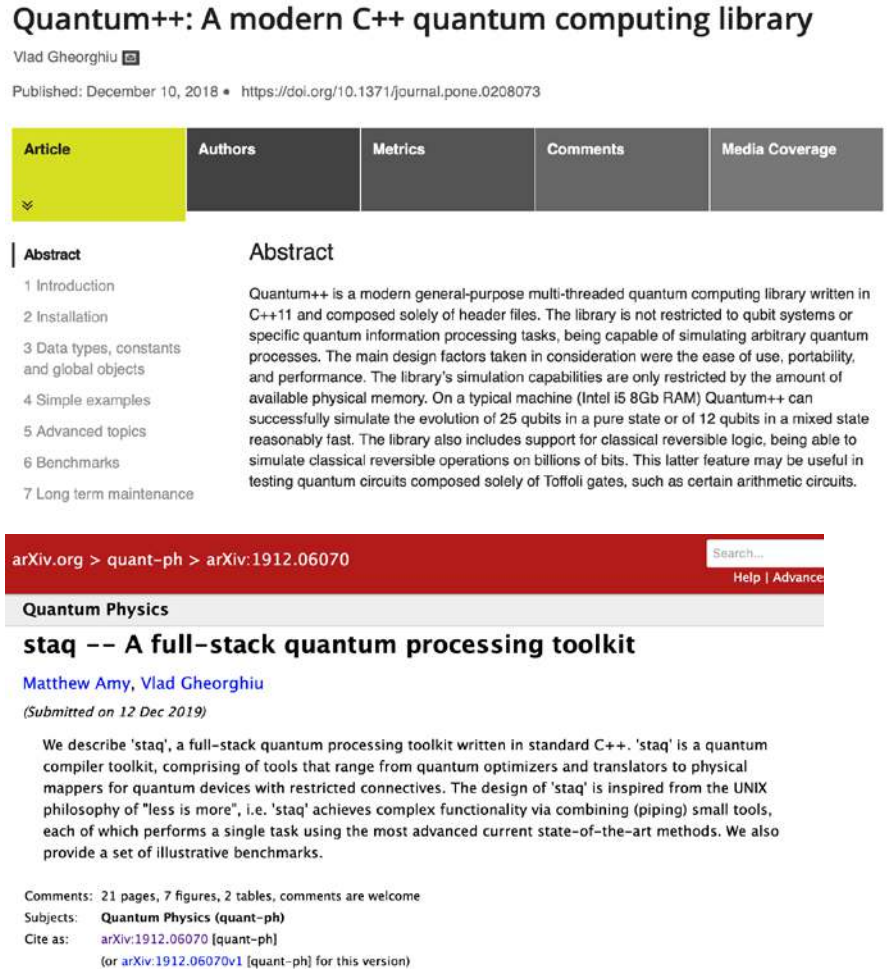
PLoS ONE 13(12): e0208073 (2018)

What can you do **now** with a quantum computer?

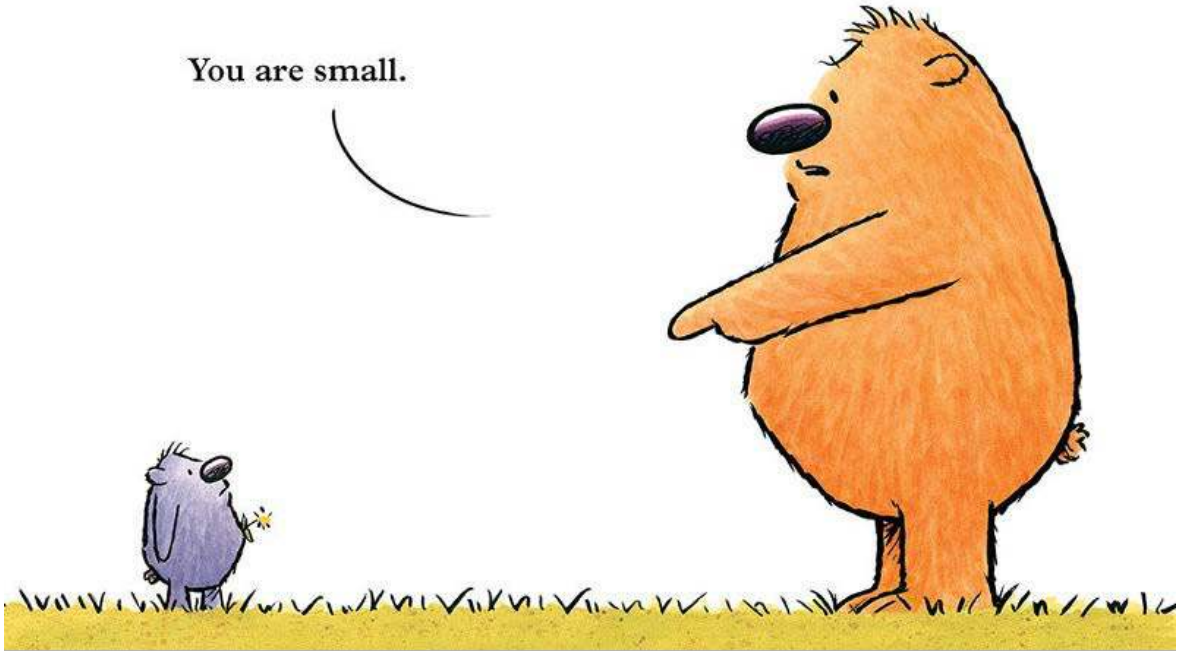
- Currently, not enough qubits for a realistic speed-up *(in circuit model)*. Proof-of-principle quantum programs.
- Main prize: understand NOW what it takes to use one and identify potential business cases, so your business will benefit ASAP once the tech is out there
- Priority: finding applications and optimizing algorithms
- Resource counts continue to decline as we improve algorithms/software; make sure you are prepared
- Plausible that in next 2-4 years (e.g. IARPA LogiQ) that a fault-tolerant qubit is demonstrated, followed by intense scaling effort
- Possible that some quantum advantage is attainable with sufficiently large NISQ devices or quantum annealers.

https://github.com/softwareQinc



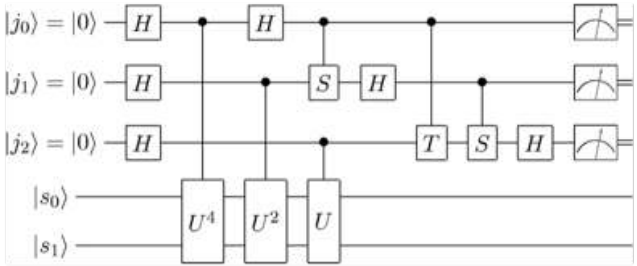


Quantum resource estimation

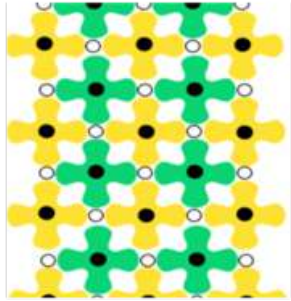


https://www.freecodecamp.org/news/asymptotic-analysis-explained-with-pokemon-a-deep-dive-into-complexity-analysis-8bf4396804e0/

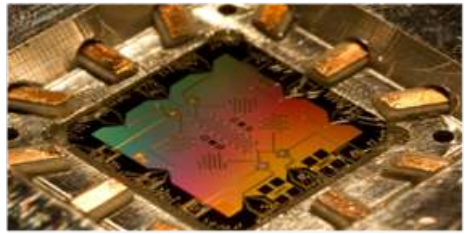
Algorithms (abstract layer)



Quantum circuits (logical layer)



Error correcting layer



Hardware (physical layer)

Discovering and implementing better circuit synthesis and optimization tools

http://qsoft.iqc.uwaterloo.ca

- Brute force exhaustive synthesis of multi-qubit unitaries
- Parallel collision-finding algorithms applied to circuit synthesis

- Optimal T-depth synthesis of one-qubit unitaries

- Optimization of T-depth via matroid partitioning
- Optimizing phase polynomials via Reed-Muller decoding
- Combinatorial methods for better Pauli decompositions applicable to Variational Quantum Eigensolvers

Various architecture considerations

Quantum Physics

Quantum circuit optimizations for NISQ architectures

Beatrice Nash, Vlad Gheorghiu, Michele Mosca

(Submitted on 3 Apr 2019 (v1), last revised 22 Apr 2019 (this version, v2))

Currently available quantum computing hardware platforms have limited 2-qubit connectivity among their addressable qubits. In order to run a generic quantum algorithm on such a platform, one has to transform the initial logical quantum circuit describing the algorithm into an equivalent one that obeys the connectivity restrictions.
In this work we construct a circuit synthesis scheme that takes as input the qubit connectivity graph and a quantum circuit over the gate set generated by $\{\mathrm{CNOT}, R_Z\}$ and outputs a circuit that respects the connectivity of the device. As a concrete application, we apply our techniques to Google's Bristlecone 72-qubit quantum chip connectivity, IBM's Tokyo 20-qubit quantum chip connectivity, and Rigetti's Acorn 19-qubit quantum chip connectivity. In addition, we also compare the performance of our scheme as a function of sparseness of randomly generated quantum circuits.
Note: Recently, the authors of arXiv:1904.00633 independently presented a similar optimization scheme. Our work is independent of arXiv:1904.00633, being a longer version of the seminar presented by Beatrice Nash at the Dagstuhl Seminar 18381: Quantum Programming Languages, pg. 120, September 2018, Dagstuhl, Germany, slide deck available online at this https URL.

To appear in Quantum Science and Technology

Quantum Physics

Fault tolerant resource estimation of quantum random-access memories

Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca

(Submitted on 4 Feb 2019)

Quantum random-access look-up of a string of classical bits is a necessary ingredient in several important quantum algorithms. In some cases, the cost of such quantum random-access memory (qRAM) is the limiting factor in the implementation of the algorithm. In this paper we study the cost of fault-tolerantly implementing a qRAM. We construct generic families of circuits which function as a qRAM, and analyze their resource costs when embedded in a surface code.

Comments: 17 pages, 12 figures. Code repository available in references
Subjects: **Quantum Physics (quant-ph)**
Cite as: arXiv:1902.01329 [quant-ph]
(or arXiv:1902.01329v1 [quant-ph] for this version)

To appear in IEEE Trans. Quantum Eng.

Bottom line for RSA-2048

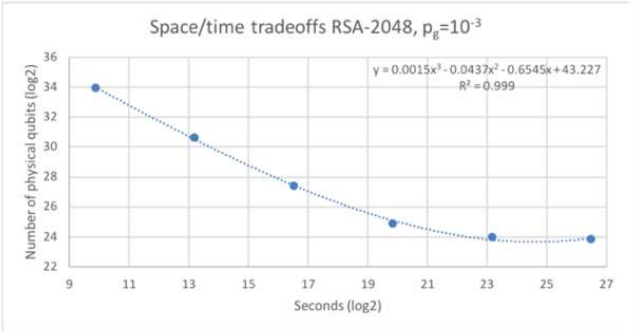
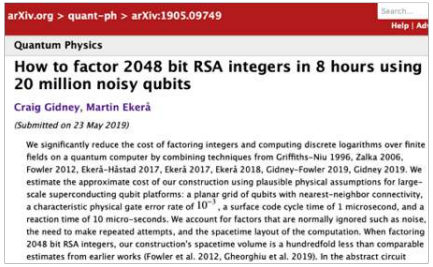


Fig. 4. RSA-2048 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.72 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.41×10^{12}, the corresponding number of logical qubits is 4098, and the total number of surface code cycles is 4.69×10^{14}. The classical security parameter is approximately 112 bits.

RSA-2048 – GIDNEY & EKERÅ UPDATES



no. of physical qubits reduced by ~10^2

	Physical assumptions				Approach		Estimated costs		
Historical cost estimate at $n = 2048$	Physical gate error rate	Cycle time (microseconds)	Reaction time (microseconds)	Physical connectivity	Distillation strategy	Execution strategy	Physical qubits (millions)	Expected runtime (days)	Expected volume (megaqubitdays)
Fowler et al. 2012 [9]	0.1%	1	0.1	planar	1200 T	single threaded	1000	1.1	1100
O'Gorman et al. 2017 [10]	0.1%	10	1	arbitrary	block CCZ	single threaded	230	3.7	850
Gheorghiu et al. 2019 [19]	0.1%	0.2	0.1	planar	1100 T	single threaded	170	1	170
(ours) 2019 (1 factory)	0.1%	1	10	planar	1 CCZ	serial distillation	16	6	90
(ours) 2019 (1 thread)	0.1%	1	10	planar	14 CCZ	single threaded	19	0.36	6.6
(ours) 2019 (parallel)	**0.1%**	**1**	**10**	**planar**	**28 CCZ**	**double threaded**	**20**	**0.31**	**5.9**

TABLE II. Historical estimates of the expected costs of factoring $n = 2048$ bit RSA integers, and the assumptions they used. Our spacetime volumes can be directly compared to the volume from Fowler et al. (we achieve a 165x improvement), because Fowler et al's estimate is dominated by distillation and changing the reaction time doesn't affect this volume. It is unclear how to compare O'Gorman et al.'s volume to ours, because of the difference in connectivity. Multiplying the volume from Gheorghiu et al. by 5, to account for the difference in cycle time, allows comparison to our volume (we achieve a 140x improvement). See Appendix B for details on each entry in this table.

On some alternative quantum factoring approaches…

Factoring semi-primes with (quantum) SAT-solvers

Michele Mosca*[1] and Sebastian R. Verschoor†[2]

and question the practical effectiveness of this approach for factoring large numbers. We find no evidence that this is a viable path toward factoring large numbers, even for scalable fault-tolerant quantum computers, as well as for various quantum annealing or other special purpose quantum hardware.

https://arxiv.org/pdf/1902.01448.pdf

On speeding up factoring with quantum SAT solvers

Michele Mosca[1], João Marcos Vensi Basso*[2], and Sebastian R. Verschoor[3]

We present a SAT circuit that can be given to quantum SAT solvers such as annealers in order to perform this step of factoring. If quantum SAT solvers achieve any speedup over classical brute-force search, then our factoring algorithm is faster than the classical NFS.

https://arxiv.org/pdf/1910.09592.pdf

A low-resource quantum factoring algorithm

Daniel J. Bernstein[1,2], Jean-François Biasse[3], and Michele Mosca[4,5,6]

heuristics, is $L^{p+o(1)}$ where $p > 1.9$. The new time complexity is asymptotically worse than Shor's algorithm, but the qubit requirements are asymptotically better, so it may be possible to physically implement it sooner.

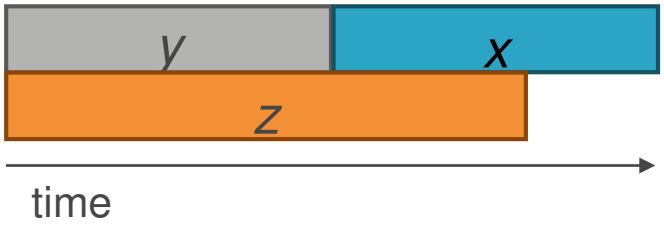
https://eprint.iacr.org/2017/352

Do we need to worry *now*?

Depends on*:

- *security shelf-life* (*x* years)
- *migration time (y years)*
- *collapse time (z years)*

"Theorem": If $x + y > z$, then worry.




ZDNet

IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'

Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years

*M. Mosca: e-Proceedings of 1st ETSI Quantum-Safe Cryptography Workshop, 2013. Also http://eprint.iacr.org/2015/1075

A very recent milestone

"Quantum supremacy"

nature

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510 (2019) | Download Citation

2139 Altmetric | Metrics »

Google claims it has achieved 'quantum supremacy' – but IBM disagrees

Task that would take most powerful supercomputer 10,000 years 'completed by quantum machine in minutes'

Critical Future Milestone:
Scalable fault-tolerant logical qubits

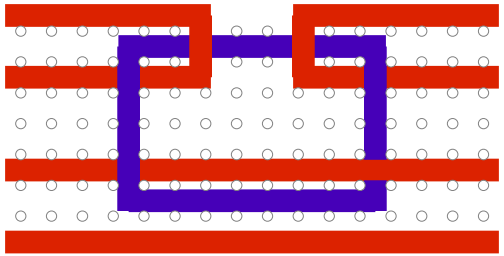
Logical layer

Physical layer

CNOT

=

fault-tolerant CNOT



Estimating ‘z’?

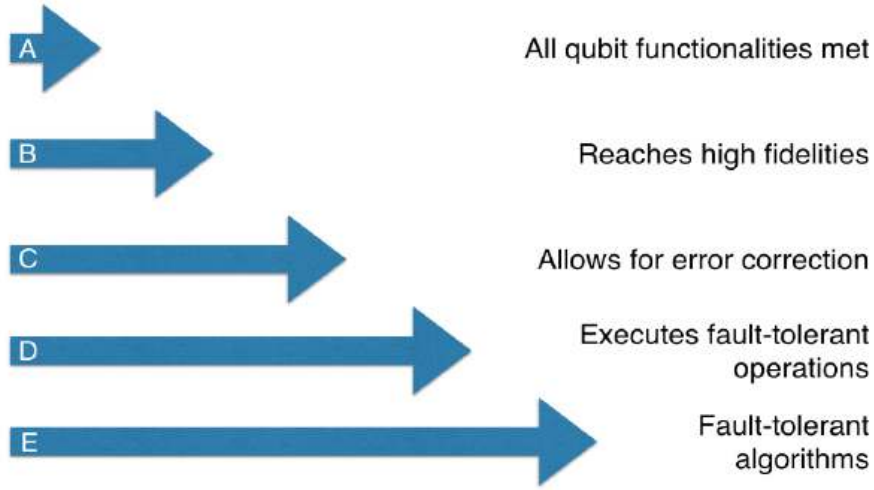
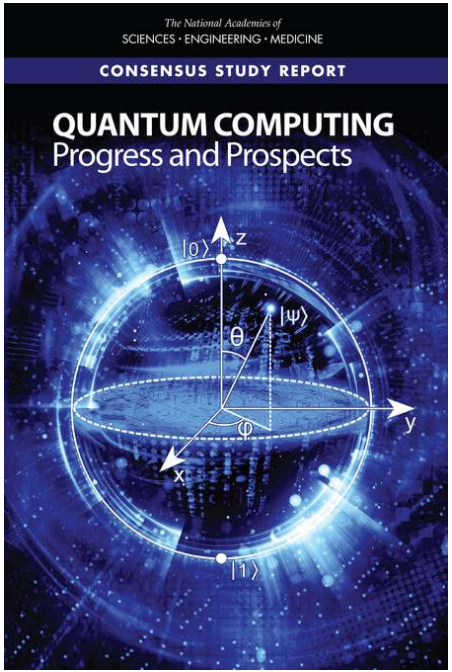


Figure 2.1: Levels of development towards a fault-tolerant quantum computer

https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer.html
(first draft in 2018; updated version 1.1 in 2019)



https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects (presented in Dec. 2018)

Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade. (Chapter 7)

Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster. (Chapter 7)

What is ‘z’?

- **Michele Mosca** [Oxford, 1996]: *“20 qubits in 20 years”*
- **Microsoft Research** [October 2015]: *”Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer* **within a decade**”*.*
- **Michele Mosca** ([NIST, April 2015], [ISACA**,** September 2015]): *“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”*
- **Michele Mosca** [London, September 2017]*: “1/6 chance within 10 years”*
- **Simon Benjamin** [London, September 2017]: *Speculates that if someone is willing to “go Manhattan project” then “maybe 6-12 years”*
- **Michele Mosca** [Seattle, November 2019]: ***1/5 chance within 10 years***

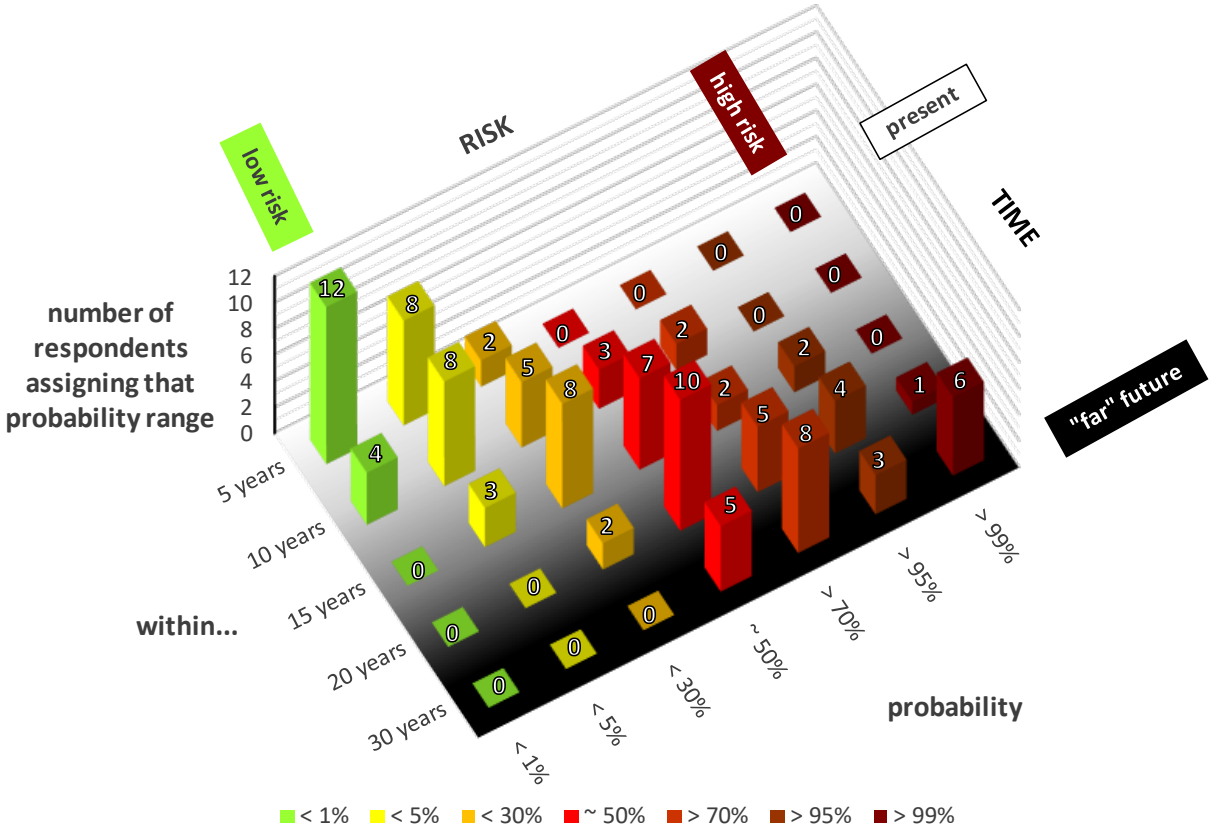
See also: https://globalriskinstitute.org/publications/quantum-threat-timeline/

Name	Institution
Scott Aaronson	University of Texas at Austin
Dorit Aharonov	The Hebrew University of Jerusalem
Dave Bacon	Google
Simon Benjamin	University of Oxford
Alexandre Blais	Université de Sherbrooke
Ignacio Cirac	Max Planck Institute of Quantum Optics
Bill Coish	McGill University
David DiVincenzo	Forschungszentrum Jülich
Runyao Duan	Institute for Quantum Computing, Baidu Research
Martin Ekerå	KTH Royal Institute of Technology and Swedish NCSA
Artur Ekert	University of Oxford and National University of Singapore

Name	Institution
Daniel Gottesman	Perimeter Institute for Theoretical Physics and Quantum Benchmark Inc
Jungsang Kim	Duke University
Ashley Montanaro	University of Bristol
Andrea Morello	UNSW Sydney
Yasunobu Nakamura	The University of Tokyo
Tracy Northup	University of Innsbruck
Peter Shor	Massachusetts Institute of Technology
Stephanie Simmons	Simon Fraser University
Krysta Svore	Microsoft
Frank Wilhelm-Mauch	Saarland University
Shengyu Zhang	Tencent

See also: https://globalriskinstitute.org/publications/quantum-threat-timeline/

Likelihood of a digital quantum computer able to break RSA-2048 in 24 hours as function of time



So what do we do about it now?

“Execution is 90% planning and 10% doing”

We don’t get to call a “time-out” if we’re not ready!

Quantum Risk Assessment (QRA) Methodology:

Phase 1- Identify and document assets, and their current cryptographic protection.

Phase 2- Research the state of emerging quantum technologies, and the timelines for availability of quantum computers.

Phase 3- Identify and document threat actors, and estimate their time to access quantum technology "**z**".

Phase 4- Identify the lifetime of your assets "**x**", and "**y**" the time required to migrate the organizations technical infrastructure to a quantum-safe state.

Phase 5- Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. (**x + y > z** ?)

Phase 6- Identify and prioritize the activities required to maintain awareness, and to migrate the organization's technology to a quantum-safe state.

https://globalriskinstitute.org/publications/3423-2/

Design issues for hybrid key exchange in TLS 1.3

Douglas Stebila, Scott Fluhrer, Shay Gueron. **Design issues for hybrid key exchange in TLS 1.3**. **Internet-Draft**. Internet Engineering Task Force, July 2019.
https://tools.ietf.org/html/draft-stebila-tls-hybrid-design-01

Thanks to Douglas Stebila for this slide.

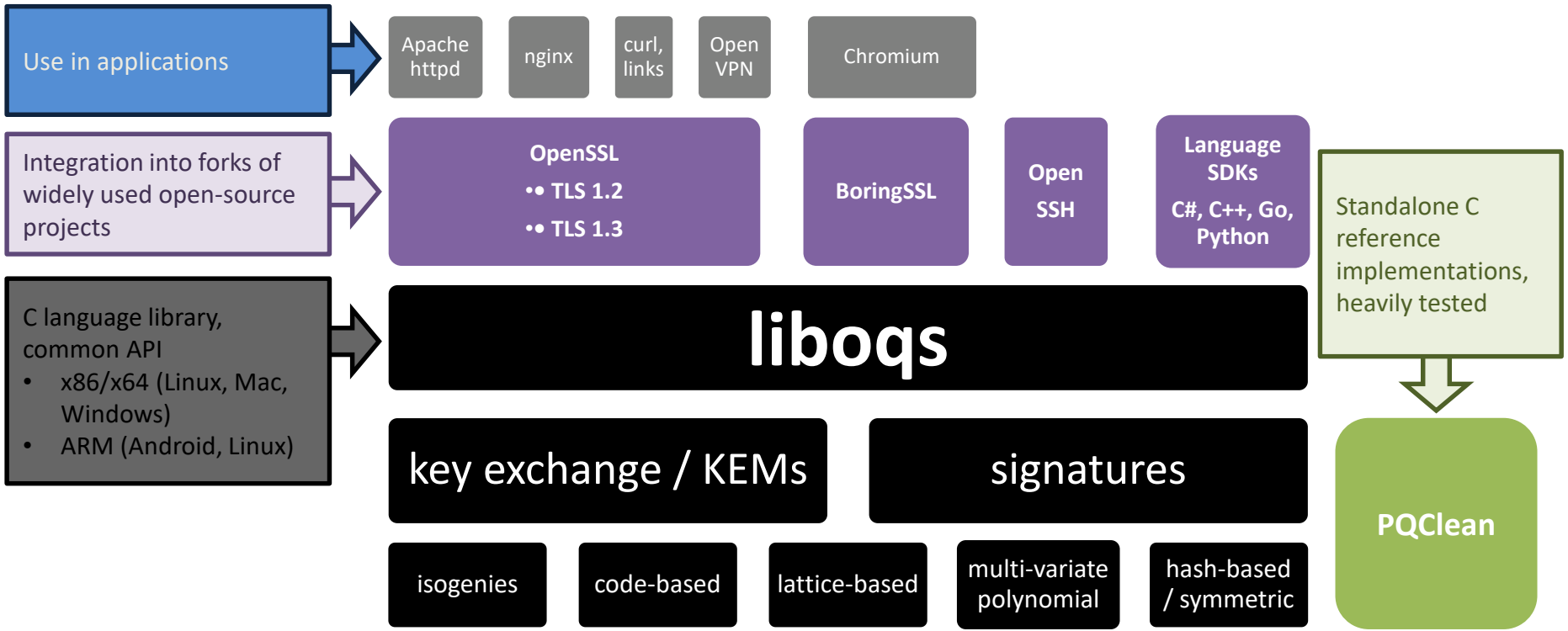
Hybrid key encapsulation mechanisms and authenticated key exchange

Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, Douglas Stebila. **Hybrid key encapsulation mechanisms and authenticated key exchange**. In Jintai Ding, Rainer Steinwandt, editors, *Proc. 10th International Conference on Post-Quantum Cryptography (PQCrypto) 2019*, *LNCS*. Springer, May 2019. https://eprint.iacr.org/2019/858

Thanks to Douglas Stebila for this slide.

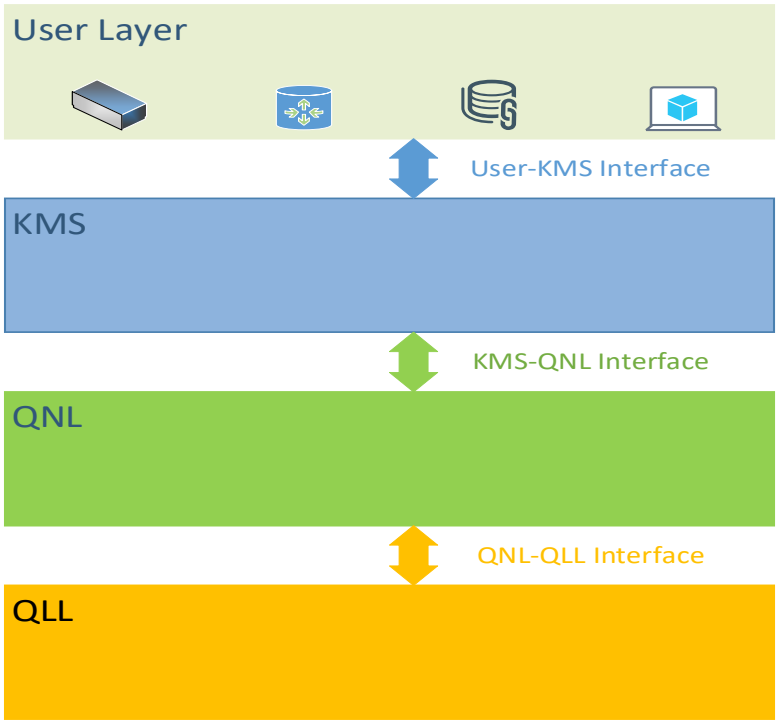
https://openquantumsafe.org/ • https://github.com/open-quantum-safe/

Open Quantum Safe Project



Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH

Eric Crockett, Christian Paquin, Douglas Stebila. **Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH**. In *NIST 2nd Post-Quantum Cryptography Standardization Conference 2019*. August 2019. https://eprint.iacr.org/2019/858


User Layer
User-KMS Interface
KMS
KMS-QNL Interface
QNL
QNL-QLL Interface
QLL

Lifecycle management vs crisis management

	Proactive	Reactive
Short term net cost (<12 months)	≈$0 (planning)	$0

Lifecycle management vs crisis management

	Proactive	Reactive
Short term net cost (<12 months)	≈$0 (planning)	$0
Short to Medium term net cost (≈1-2 years)	≈$0 (planning/testing/ vendor dialogue)	≈$0 (potential loss of customers)

Lifecycle management vs crisis management

	Proactive	Reactive
Short term net cost (<12 months)	≈$0 (planning)	$0
Short to Medium term net cost (≈1-2 years)	≈$0 (planning/testing/ vendor dialogue)	≈$0 (potential loss of customers)
Medium to Long term net cost (≈3-8 years)	≈$0 (updating/testing/vendor selection) +potential gain of customers	Likely substantial costs (increasingly likely loss of customers; potential non-compliance with emerging regulations; rushed replacement of software/hardware)

Lifecycle management vs crisis management

	Proactive	Reactive
Short term net cost (<12 months)	≈$0 (planning)	$0
Short to Medium term net cost (≈1-2 years)	≈$0 (planning/testing/ vendor dialogue)	≈$0 (potential loss of customers)
Medium to Long term net cost (≈3-8 years)	≈$0 (updating/testing/vendor selection) +potential gain of customers	Likely substantial costs (increasingly likely loss of customers; potential non-compliance with emerging regulations; rushed replacement of software/hardware)
Long term net cost	Net gains (new customers and **better security against conventional attacks**)	Ranges from substantial to devastating (loss of past and present data; collapse of systems due to cryptanalysis, loss of trust, lack of interoperability, etc.) **Large potential costs also to customers and the broader ecosystem**

2020 Resolutions

- Put someone in charge of producing a quantum readiness plan by Q3
- Provide them broad executive support for the planning exercise
- Give NIST feedback on cryptographic algorithm requirements by April 2020
- Update RFPs and start/continue vendor engagement by Q4

Well done!

Great progress in the past year.

Let's keep going!

More to do in the coming year.

Thank you!

Comments, questions and feedback are very welcome.

Michele Mosca
Professor, Faculty of Mathematics
Co-Founder, Institute for Quantum Computing,
University of Waterloo www.iqc.ca/~mmosca
mmosca@uwaterloo.ca

CEO, evolutionQ Inc. @evolutionQinc
michele.mosca@evolutionq.com

Co-founder, softwareQ Inc. softwareq.ca