Update on the quantum threat and mitigation timelines and managing quantum risk

Michele Mosca

17 May 2017

CryptoWorks21

evolutionQ

University of Waterloo | IQC Institute for Quantum Computing

Perimeter Institute for Theoretical Physics

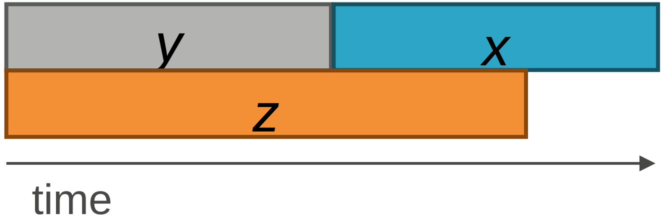
Do we need to worry *now*?

Depends on:

- X = *security shelf-life*
- Y = *migration time*
- Z = *collapse time*

“Theorem”: If *X* + *Y* > *Z*, then worry.

EPRINT.IACR.ORG/2015/1075



Bottom line

Fact: If X+Y>Z, then you will not be able to provide the required X years of security.

Fact: If Y>Z then cyber systems will collapse in Z years with no quick fix.

Fact: Rushing “Y” will be expensive, disruptive, and lead to vulnerable implementations.

Prediction: In the next 6-24 months, organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan.

Toward estimating “z”

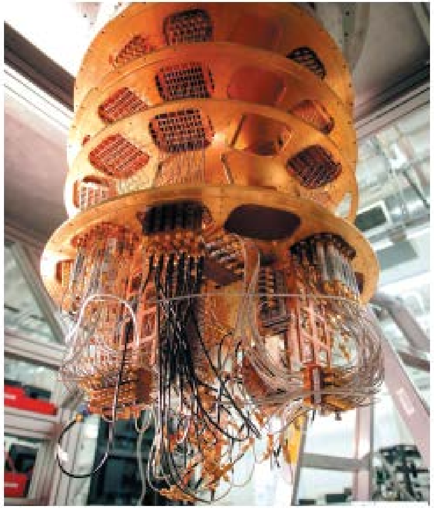
- E.g. What resources are required to break RSA-2048?
- A billion qubits and a trillion gates?
- A million qubits and 100 million gates?
- Something else?
- Asymptotic complexity estimates give a very coarse-grained approximation.
- To attempt to estimate this question, we need a more fine-grained study of the full tool chain between algorithms and physical qubits.

Scalable fault-tolerant quantum computer

- Known to solve many problems previously thought to be intractable
- Simulating quantum systems (optimizing/designing materials, drugs, chemical processes, etc)
- Optimization (resource allocation, process design, etc.)
- Computational mathematics (including breaking current public-key cryptography)
- and more…

Non-fault-tolerant quantum devices

- *Not a known threat to cryptography*
- Can they capture *some* of the power of quantum computation (and bypass some/all the cost of fault-tolerance)?
- Can they simulate themselves or similar systems faster/cheaper than conventional computers?
- Can they solve *useful* problems better than conventional devices?



Google's cryostats reach temperatures of 10 millikelvin to run its quantum processors.

Commercialize early quantum technologies

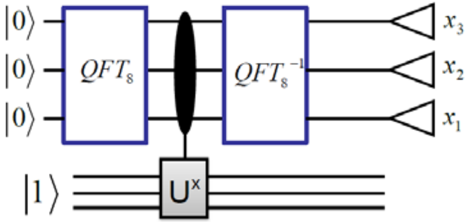
Masoud Mohseni, Peter Read, Hartmut Neven and colleagues at Google's Quantum AI Laboratory set out investment opportunities on the road to the ultimate quantum machines.

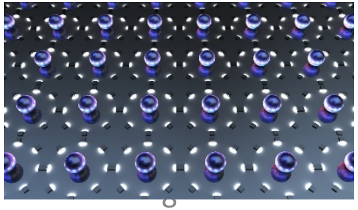
MARCH 2017 | VOL 543 | NATURE | 171

"Similarly, although there is no proof today that imperfect quantum machines can compute fast enough to solve practical problems, that may change."

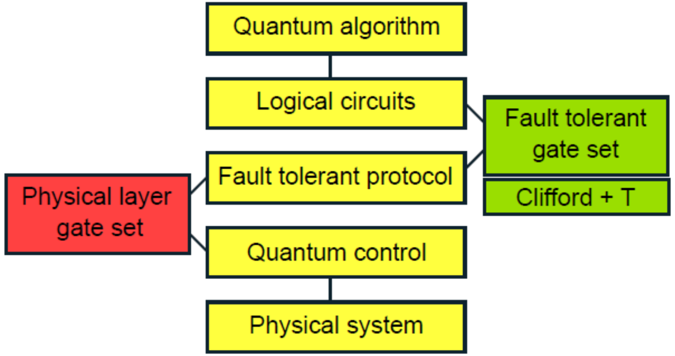
What logical layer quantum resources are needed?

- Algorithm modifications and optimizations can reduce qubit requirement and/or circuit size, e.g.
  - Only one control qubit needed for eigenvalue estimation (Mosca-Ekert ‘98)
  - Mixed state target register suffices (Mosca ‘99)
  - Weaker phase estimates suffice (Seifert ‘01)
  - Other reductions for DLP and factoring (Ekerå, Håstad ‘17)
  - $\tilde{O}(\log(N))^{2/3}$ logical qubits allow speed-up of NFS (Bernstein-Biasse-Mosca ‘17)


|0⟩
|0⟩
|0⟩
|1⟩
QFT8
QFT8 −1
Ux
x3
x2
x1



How large of a quantum computer is needed?



Institute for Quantum Computing » Events » 2015 » June »

Quantum Programming and Circuits Workshop

Monday, June 8, 2015 (all day) to Thursday, June 11, 2015 (all day)

The workshop aims at bringing together researchers from quantum computing and classical programming languages. Open questions that we anticipate this group to tackle include new methods for circuit synthesis and optimization, compiler optimizations and rewriting, embedded languages versus non-embedded languages, implementations of type systems and error reporting for quantum languages, techniques for verifying the correctness of quantum programs, and new techniques for compiling efficient circuits and protocols for fault-tolerant questions and their 2D layout.

https://qsoft.iqc.uwaterloo.ca/

(Quantum Compiler tools,
Quantum Computer Simulator – Quantum++ , etc.)

Some useful quantum compiler tools

- 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

PQCrypto 2016

Post-Quantum Cryptography
Volume 9606 of the series Lecture Notes in Computer Science pp 29-43

Date: 04 February 2016

Applying Grover's Algorithm to AES: Quantum Resource Estimates

Markus Grassl, Brandon Langenberg, Martin Roetteler, Rainer Steinwandt

Our AES analysis, e.g. 192-bit AES:
$5.9\text{x}10^6$ qubits,
2^{121} surface code cycles,
$2^{137.5}$ total cost

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3

Matthew Amy[1,4], Olivia Di Matteo[2,4], Vlad Gheorghiu[3,4], Michele Mosca[3,4,5,6], Alex Parent[2,4], and John Schanck[3,4]

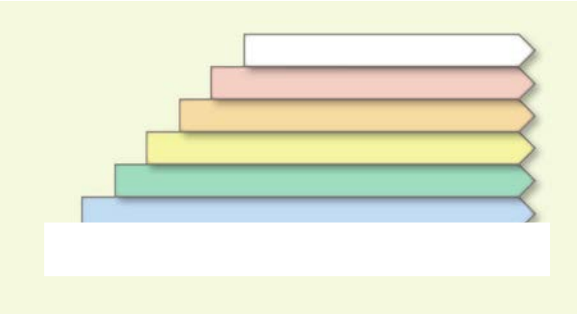
		SHA-256	SHA3-256
Grover	T-count	1.27×10^{44}	2.71×10^{44}
	T-depth	3.76×10^{43}	2.31×10^{41}
	Logical qubits	2402	3200
	Surface code distance	43	44
	Physical qubits	1.39×10^{7}	1.94×10^{7}
Distilleries	Logical qubits per distillery	3600	3600
	Number of distilleries	1	294
	Surface code distances	$\{33, 13, 7\}$	$\{33, 13, 7\}$
	Physical qubits	5.54×10^{5}	1.63×10^{8}
Total	Logical qubits	$2^{12.6}$	2^{20}
	Surface code cycles	$2^{153.8}$	$2^{146.5}$
	Total cost	$2^{166.4}$	$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

REVIEW SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

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



Science Advances AAAS

Home News Journals Topics Careers

Science Science Advances Science Immunology Science Robotics Science Signaling Science Translational Medicine

RESEARCH ARTICLE | QUANTUM COMPUTING

Blueprint for a microwave trapped ion quantum computer

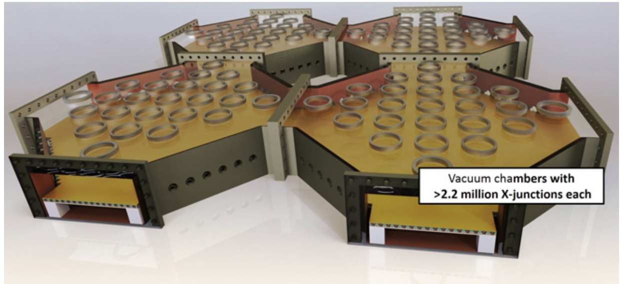
SHARE

Bjoern Lekitsch[1], Sebastian Weidt[1], Austin G. Fowler[2], Klaus Mølmer[3], Simon J. Devitt[4], Christof Wunderlich[5] and Winfried K. Hensinger[1,*]

+ Author Affiliations

*Corresponding author. Email: w.k.hensinger@sussex.ac.uk

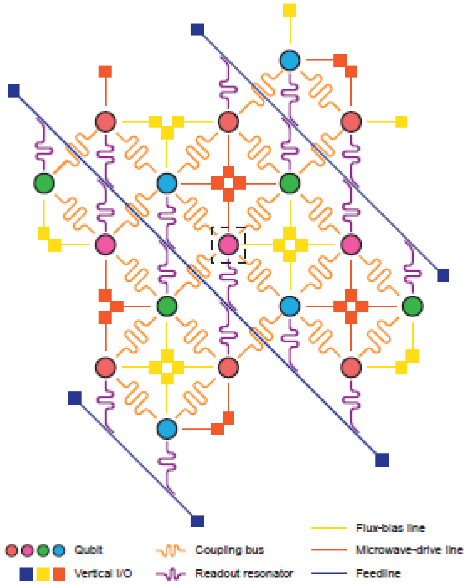
Science Advances 01 Feb 2017:
Vol. 3, no. 2, e1601540
DOI: 10.1126/sciadv.1601540



Scalable quantum circuit and control for a superconducting surface code

R. Versluis,[1,2] S. Poletto,[2,3] N. Khammassi,[4] N. Haider,[1,2]
D. J. Michalak,[5] A. Bruno,[2,3] K. Bertels,[4,3] and L. DiCarlo[2,3]

arXiv:1612.08208v1 [quant-ph] 24 Dec 2016

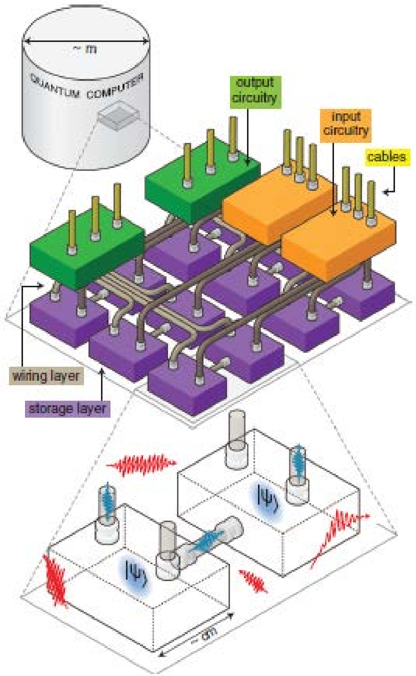


npj Quantum Information
www.nature.com/npjqi

PERSPECTIVE OPEN

Multilayer microwave integrated quantum circuits for scalable quantum computing

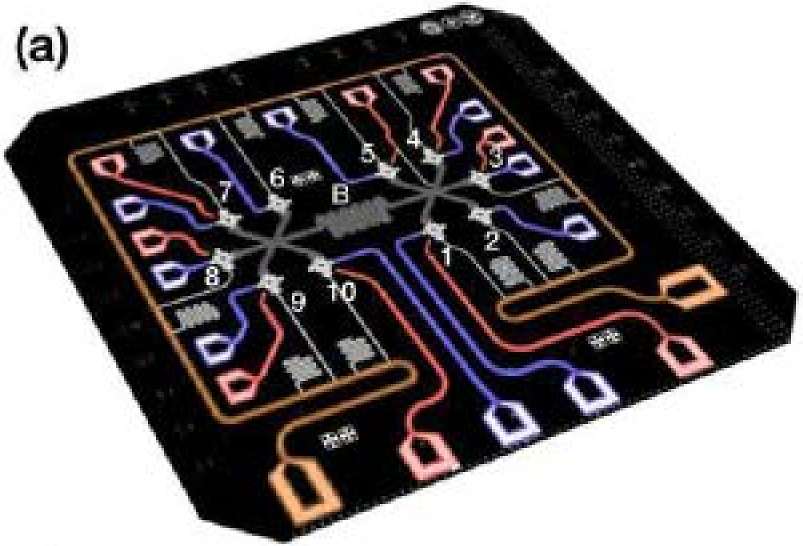
Teresa Brecht[1], Wolfgang Pfaff[1], Chen Wang[1], Yiwen Chu[1], Luigi Frunzio[1], Michel H Devoret[1] and Robert J Schoelkopf[1]



10-qubit entanglement and parallel logic operations with a superconducting circuit

Chao Song[1,2,*] Kai Xu[1,2,*] Wuxin Liu[1], Chuiping Yang[3], Shi-Biao Zheng[4,†] Hui Deng[5], Qiwei Xie[6], Keqiang Huang[5], Qiujiang Guo[1], Libo Zhang[1], Pengfei Zhang[1], Da Xu[1], Dongning Zheng[5], Xiaobo Zhu[2,‡] H. Wang[1,2,§] Y.-A. Chen[2], C.-Y. Lu[2], Siyuan Han[7], and J.-W. Pan[2]

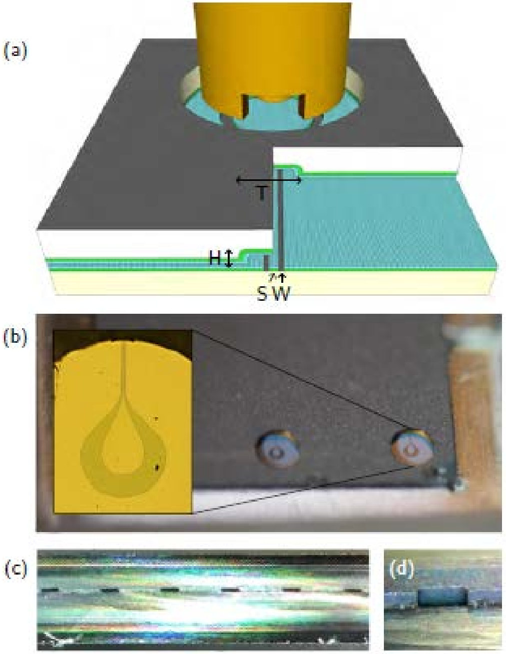
arXiv:1703.10302v1 [quant-ph] 30 Mar 2017



Thermocompression Bonding Technology for Multilayer Superconducting Quantum Circuits

C.R. H. McRae,[1,2] J. H. Béjanin,[1,2] Z. Pagel,[1,a)] A. O. Abdallah,[1,2] T. G. McConkey,[1,3] C. T. Earnest,[1,2] J. R. Rinehart,[1,2] and M. Mariantoni[1,2,b)]

arXiv:1705.02435v1 [physics.app-ph] 6 May 2017



What is ‘z’?

Mosca:
[Oxford] 1996: *“20 qubits in 20 years”*
[NIST April 2015, ISACA September 2015]:
“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”
EPRINT.IACR.ORG/2015/1075

Microsoft Research [October 2015]: *Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer* **within a decade**. *…Use of a quantum computer enables much larger and more accurate simulations than with any known classical algorithm, and will allow many open questions in quantum materials to be resolved once a small quantum computer with around* **one hundred logical qubits** *becomes available.*

Quantum-safe cryptographic tool-chest

conventional quantum-safe cryptography

a.k.a. Post-Quantum Cryptography

- Deployable without quantum technologies
- Believed/hoped to be secure against quantum computer attacks of the future

+

quantum cryptography

- Requires some quantum technologies (less than a large-scale quantum computer)
- Typically no computational assumptions and thus known to be cryptographically secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem

Quantum Risk Assessment

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 the time required to migrate the organizations technical infrastructure to a quantum-safe state "**y**".

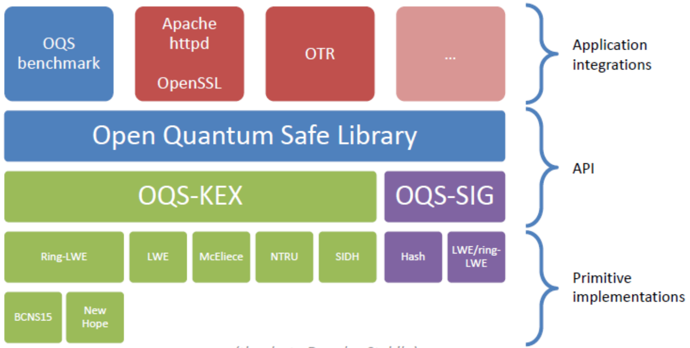
Phase 5- Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. (**x + y > z** ?)

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

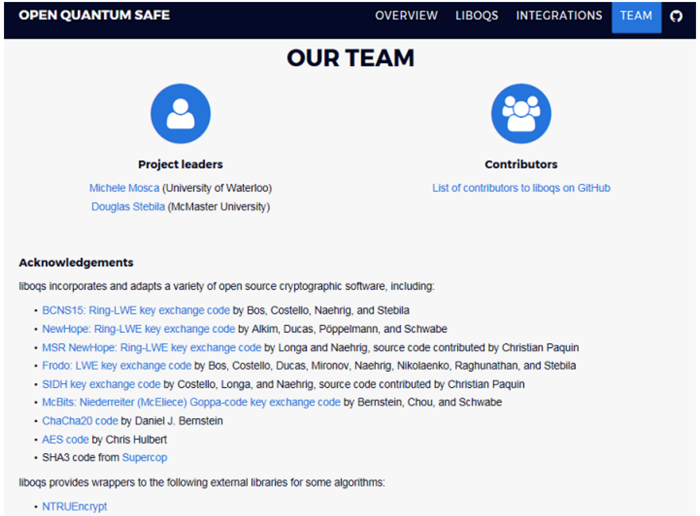
http://www.evolutionq.com/methodology-for-qra.html

Testing new tools

openquantumsafe.org



(thanks to Douglas Stebila)



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

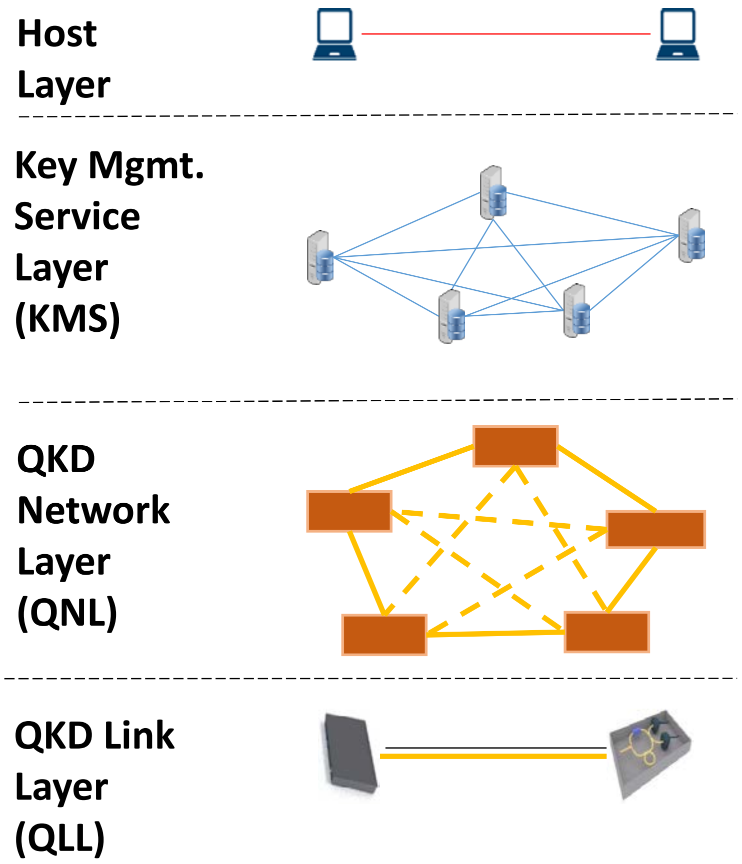
Acknowledgements

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



Full Protocol Stack for QKD

The New York Times

The Opinion Pages | CONTRIBUTING OP-ED WRITER

The World Is Getting Hacked. Why Don’t We Do More to Stop It?

Zeynep Tufekci MAY 13, 2017

If I have painted a bleak picture, it is because things are bleak. Our software evolves by layering new systems on old, and that means we have constructed entire cities upon crumbling swamps. And we live on the fault lines where more earthquakes are inevitable. All the key actors have to work together, and fast.

Security is a choice

Problematic choices:

- “Do nothing: my vendors will take care of this for me”
- “Do nothing until NIST standardization is done”
- “Get it over with”

Historic opportunity

The choice is ours

Embrace quantum technologies that will help humanity
and
live in a safer cyber-enhanced world?

Thank you!

Comments, questions and feedback are very welcome.

University Research Chair, Faculty of Mathematics
Co-Founder, Institute for Quantum Computing www.iqc.ca/~mmosca
Director, CryptoWorks21
www.cryptoworks21.com
University of Waterloo
mmosca@uwaterloo.ca

Michele Mosca
Co-founder and CEO, evolutionQ Inc.
Michele.Mosca@evolutionQ.com