sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

The quantum threat to financial services

sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

Michele Mosca

Co-Founder, Institute for Quantum Computing
University of Waterloo

evolution

CryptoWorks21

GRI | GLOBAL RISK INSTITUTE

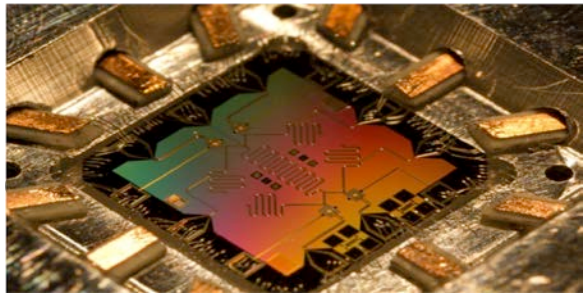
PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

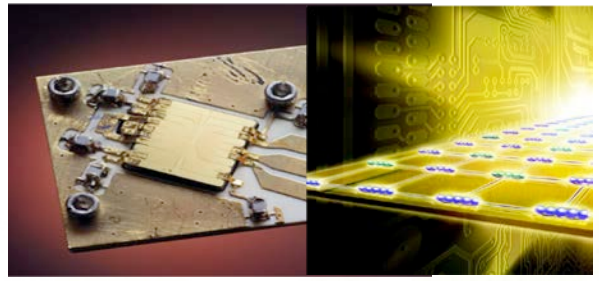
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

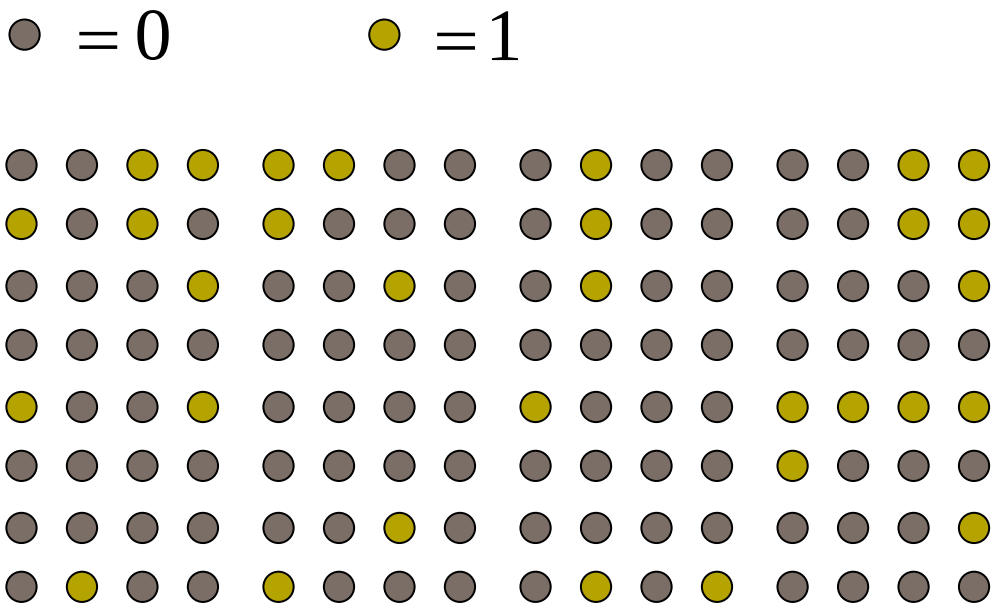
Quantum-Safe CANADA

What is a quantum computer?

- What is a *classical* computer?
- A device that encodes information in an array of bits, manipulate those bits according to simple rules



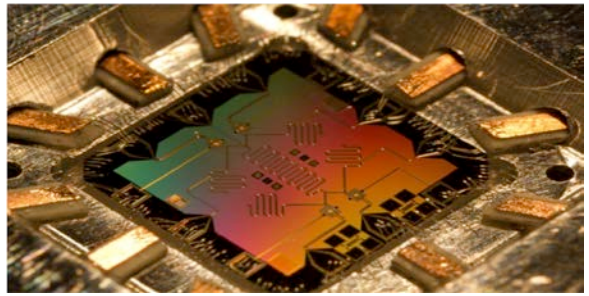


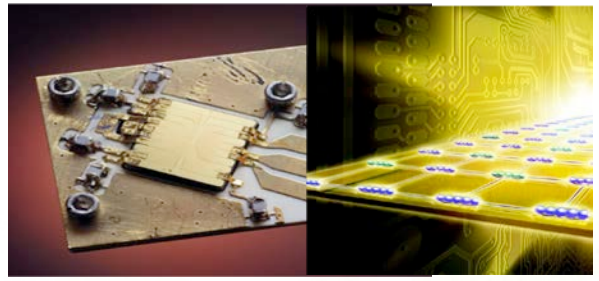


"I've always wanted to peak under the hood of one of these bad boys."

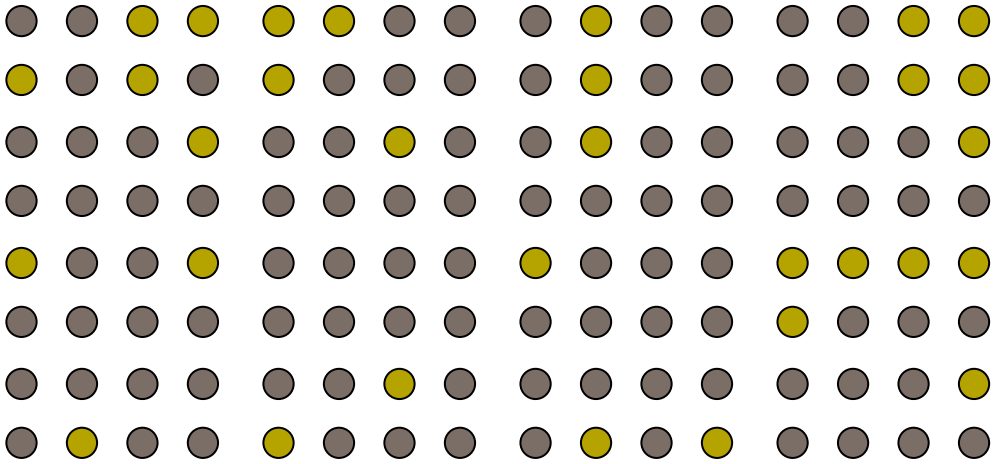
What is a quantum computer?

- What is a *quantum* computer?
- A device that encodes information in an array of bits, and can manipulate those bits according to simple quantum rules



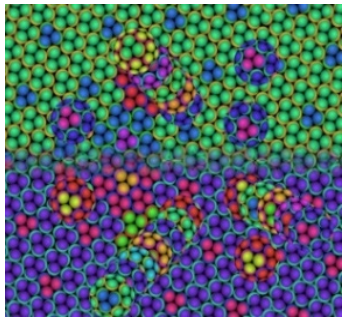


$= 0$ $= 1$

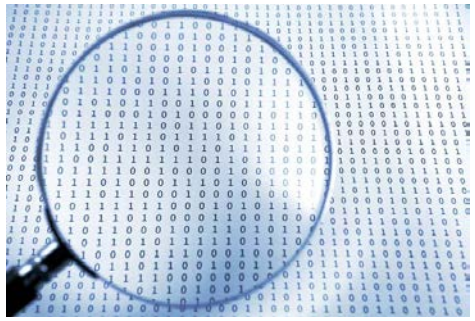


"I've always wanted to peak under the hood of one of these bad boys."

Quantum paradigm brings new possibilities



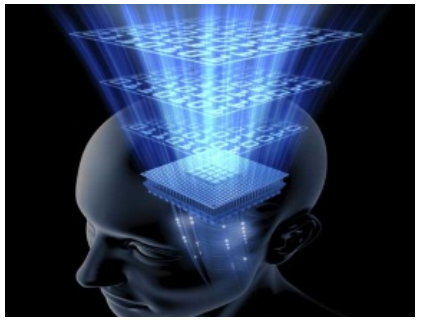
Designing new materials, drugs, etc.



Optimizing

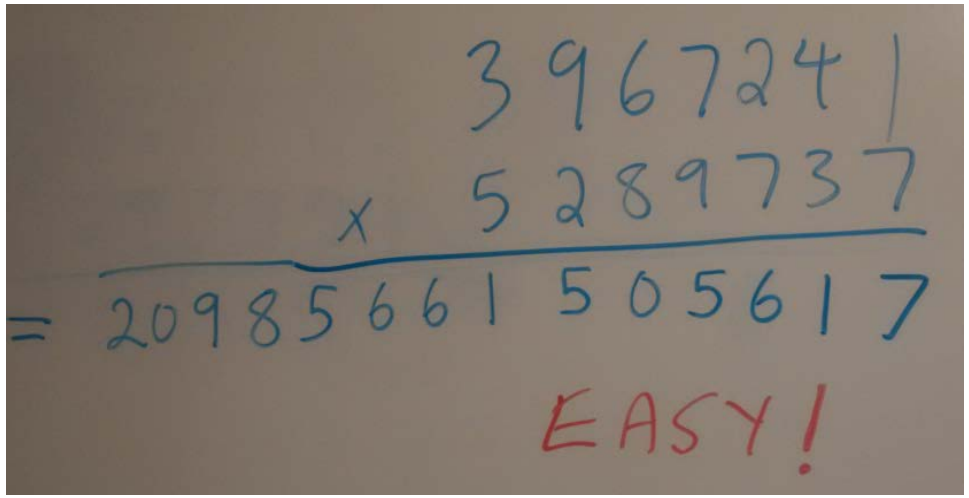
Sensing and measuring

Secure communication

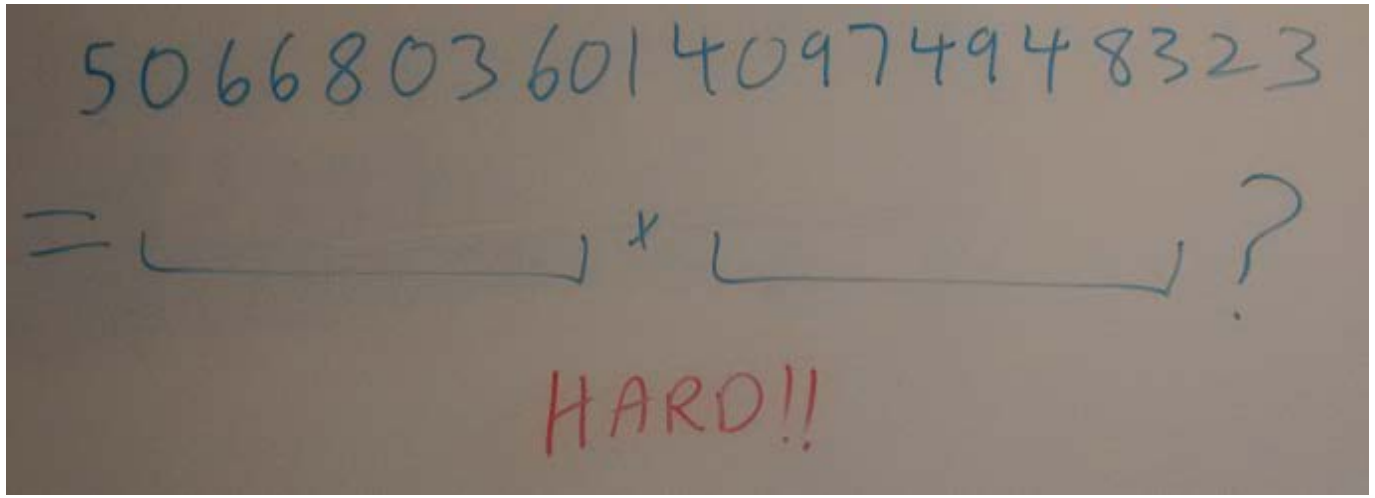


What else???

But…while in the old paradigm

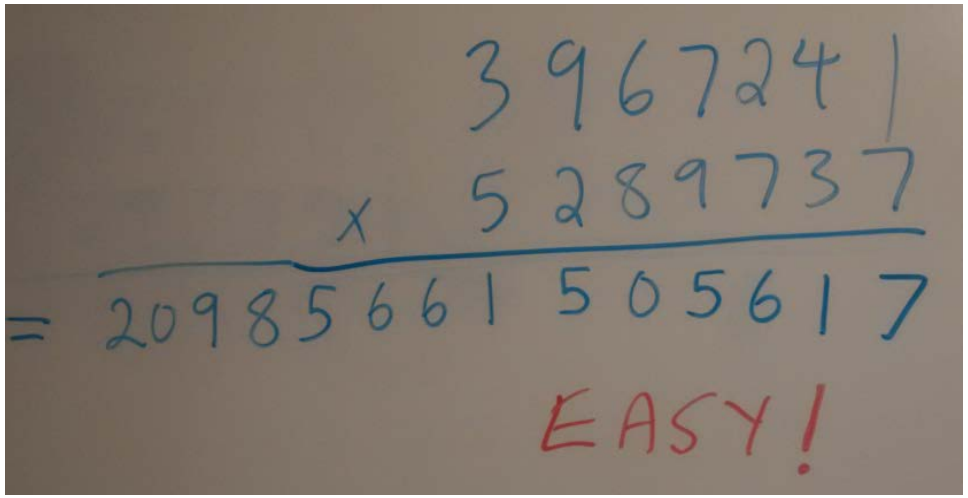


Encrypting is easy

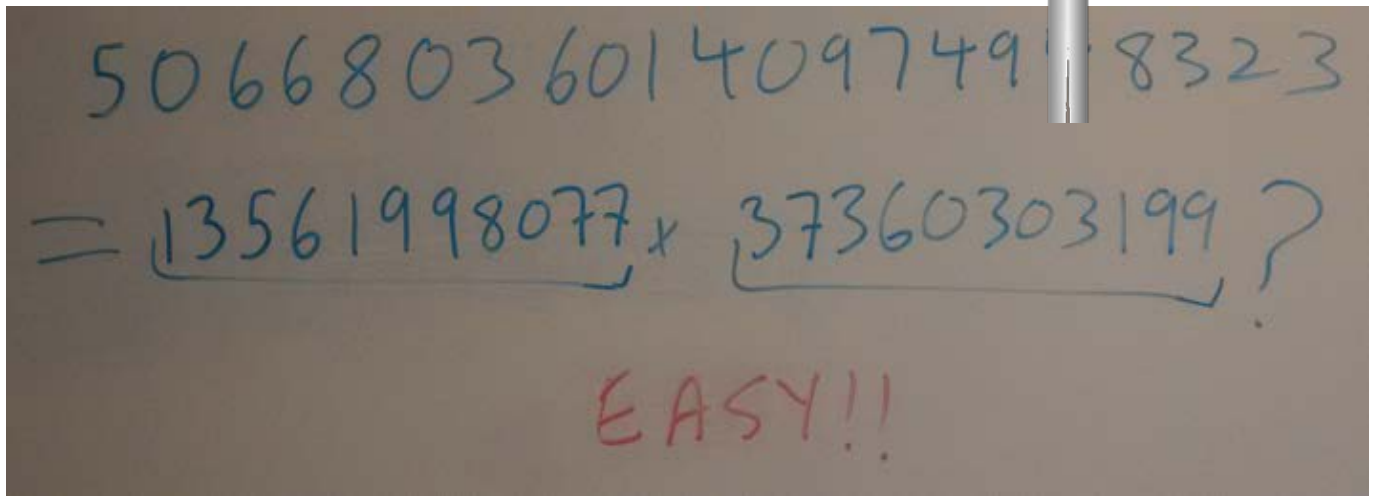


Codebreaking is hard

…in the quantum paradigm



Encrypting is easy



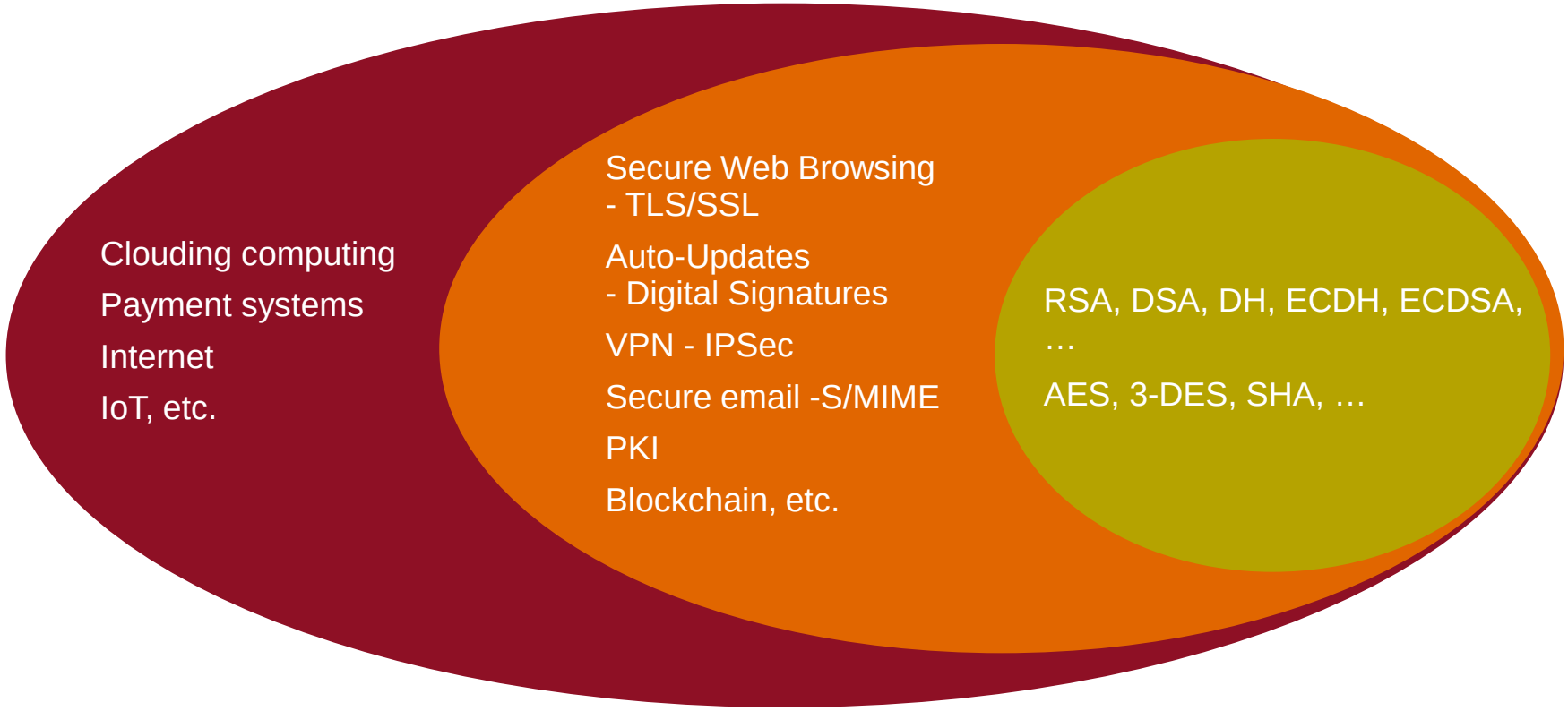
Codebreaking is easy!

How secure will our current crypto algorithms be?

Algorithm	Key Length	Security level (Conventional Computer)	Security level (Quantum Computer)
RSA-1024	1024 bits	80 bits	~0 bits
RSA-2048	2048 bits	112 bits	~0 bits
ECC-256	256 bits	128 bits	~0 bits
ECC-384	384 bits	192 bits	~0 bits
AES-128	128 bits	128 bits	~64 bits
AES-256	256 bits	256 bits	~128 bits

What will be affected?

Products, services, business functions that rely on security products will either stop functioning or not provide the expected levels of security



What will be affected?

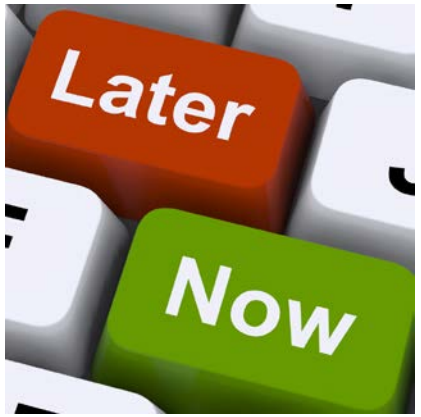
Products, services, business functions that rely on security products will either stop functioning or not provide the expected levels of security

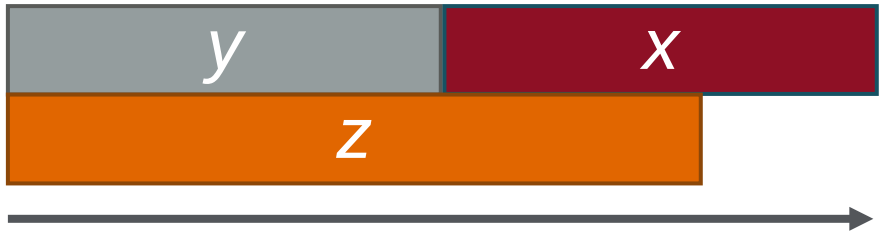
Do we need to worry now?

Depends on:

- How long do you need your cryptographic keys to be secure? - *security shelf-life* (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years) – *migration time*
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (z years) – *collapse time*

“Theorem”: If x + y > z, then worry





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

Business bottom line

Fact: If x+y>z, then you will not be able to provide the required x years of security

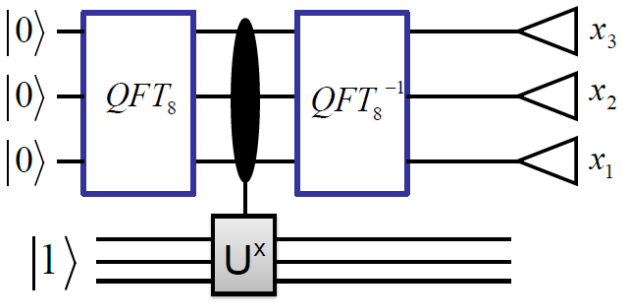
Fact: If y>z then cyber systems will collapse in z years with no quick fix

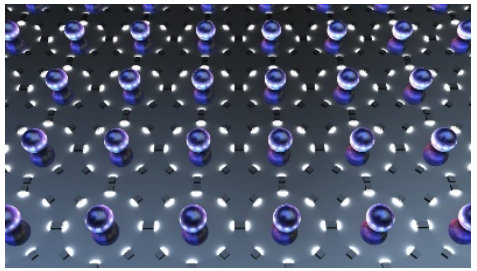
Fact: Rushing “y” will be expensive, disruptive, and lead to vulnerable implementations

Prediction: In the next 6-18 months, organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan

So what is *z* (threat timeline)?

How large of a quantum computer is needed?





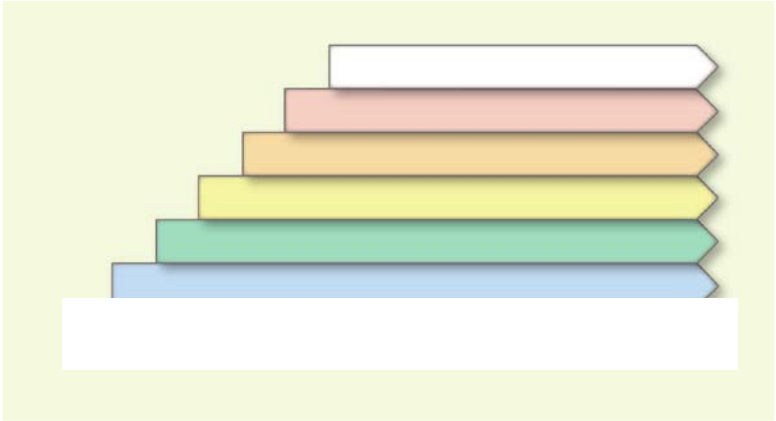
- Quantum algorithm
- Local circuits
- Fault tolerant protocol
- Quantum control
- Physical system

How close are we to having sufficient quantum resources?

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

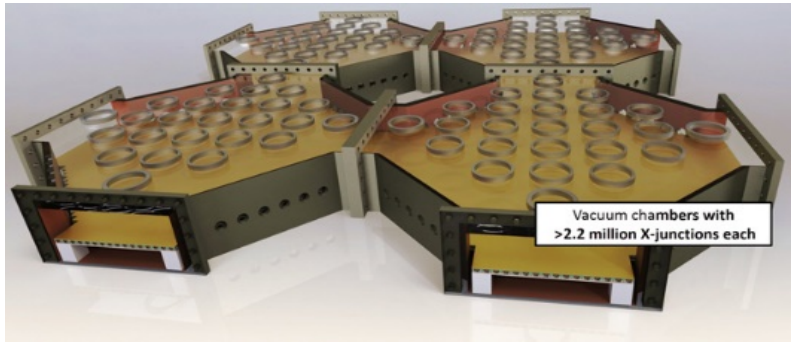
Bjoern Lekitsch[1], Sebastian Weidt[1], Austin G. Fowler[2], Klaus Mølmer[3], Simon J. Devitt[4], Christof Wunderlich[5] and Winfried K. Hensinger[1,*]

+ 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

SHARE

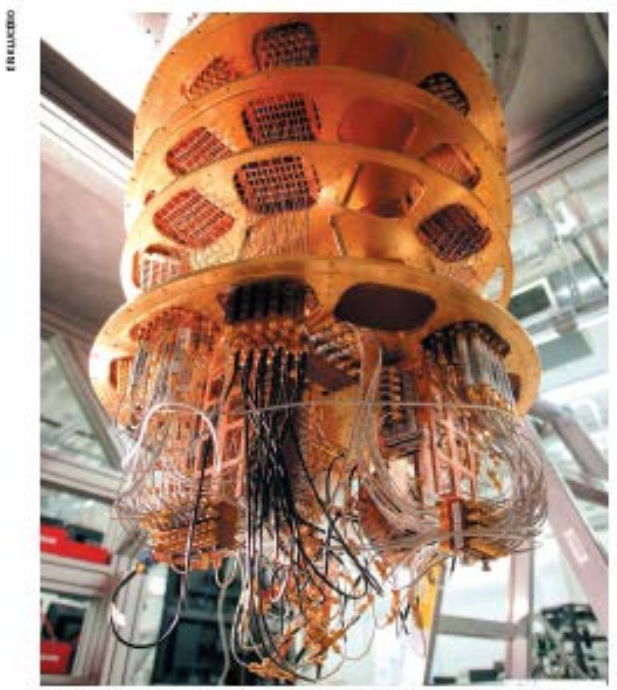


Non-fault-tolerant quantum devices

Not a known threat to cryptography

- Can they capture some of the power of quantum computation?
- Can they simulate themselves or similar systems faster/cheaper than conventional computers?
- Can they solve *useful* problems better than conventional devices?

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



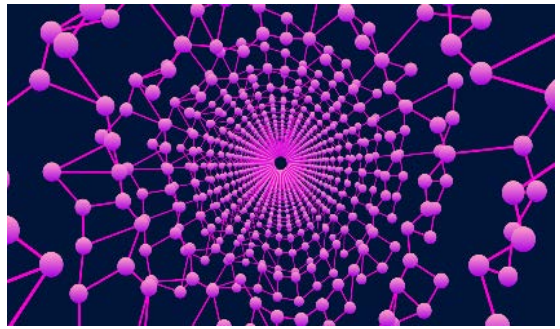
Google's cryostats reach temperatures of 10 millikelvin to run its quantum processors.

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.

Scalable fault-tolerant quantum computer

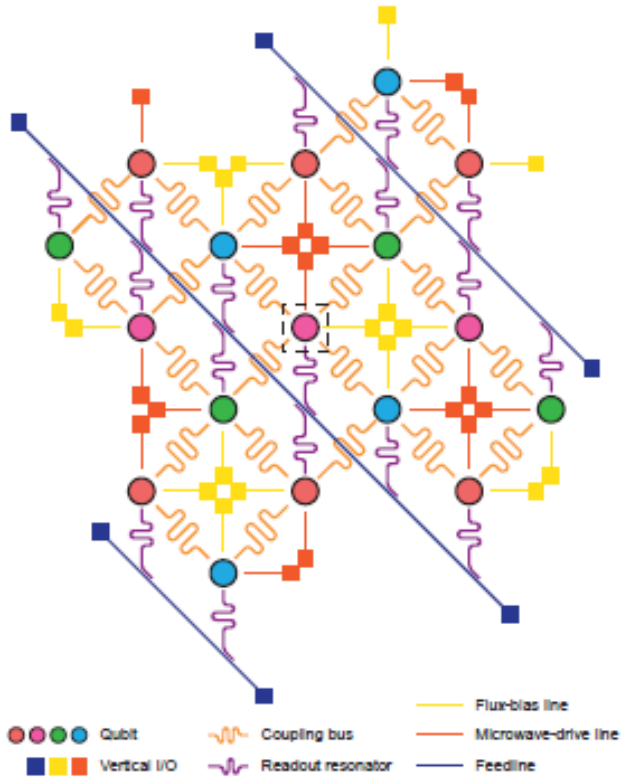
Known to solve many problems previously thought to be intractable





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]



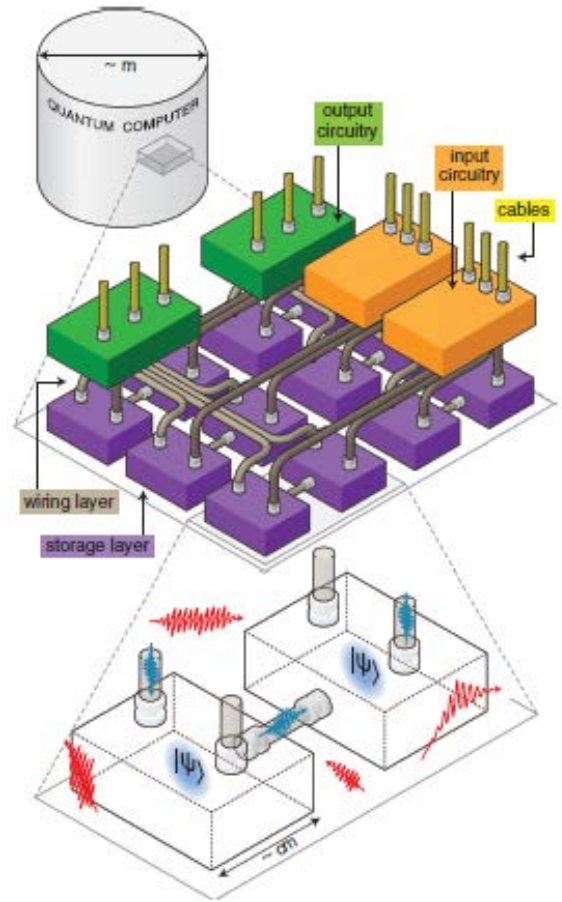
npj | Quantum Information

www.nature.com/npjqi

PERSPECTIVE OPEN

Multilayer microwave integrated quantum circuits for scalable quantum computing

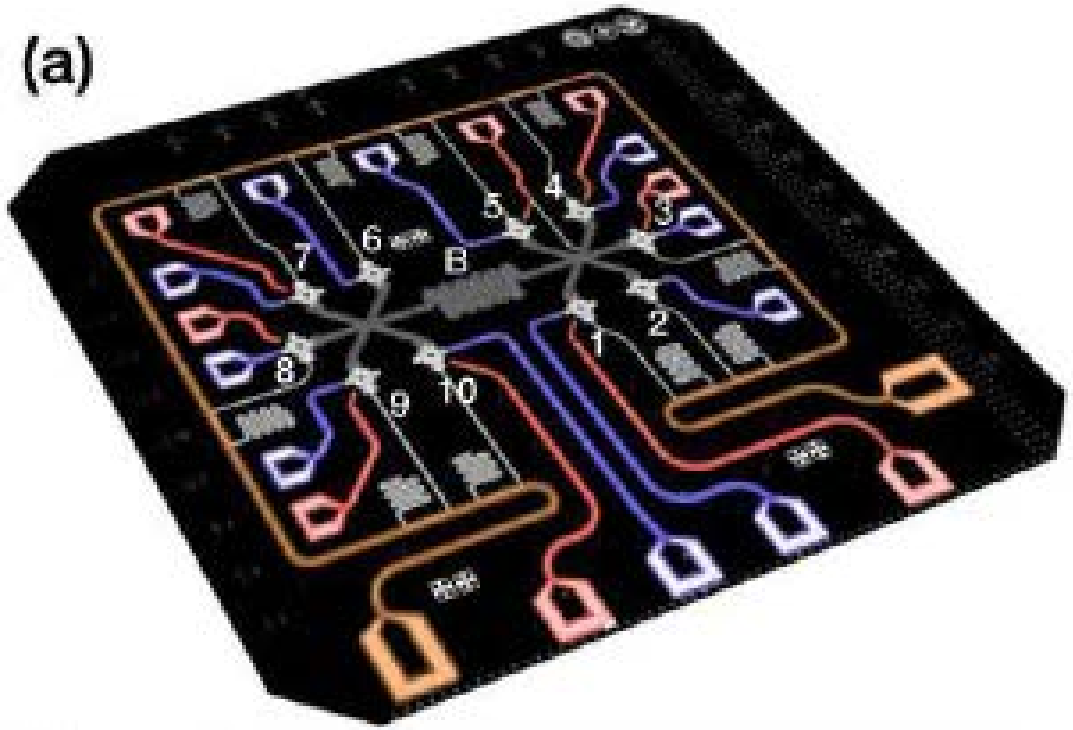
Teresa Brecht[1], Wolfgang Pfaff[1], Chen Wang[1], Yiwen Chu[1], Luigi Frunzio[1], Michel H Devoret[1] and Robert J Schoelkopf[1]



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]

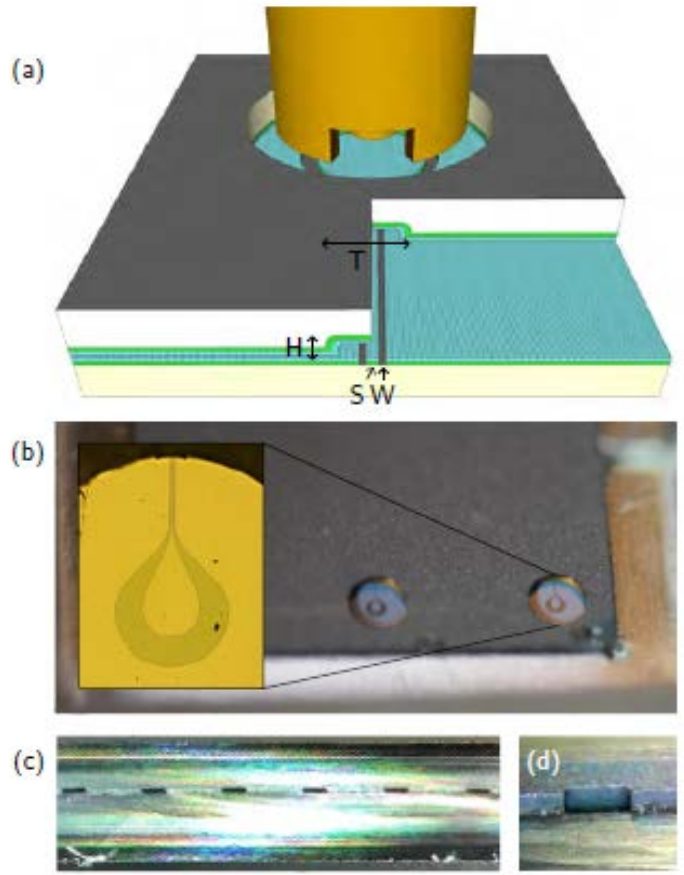
arXiv:1703.10302v1 [quant-ph] 30 Mar 2017



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)]

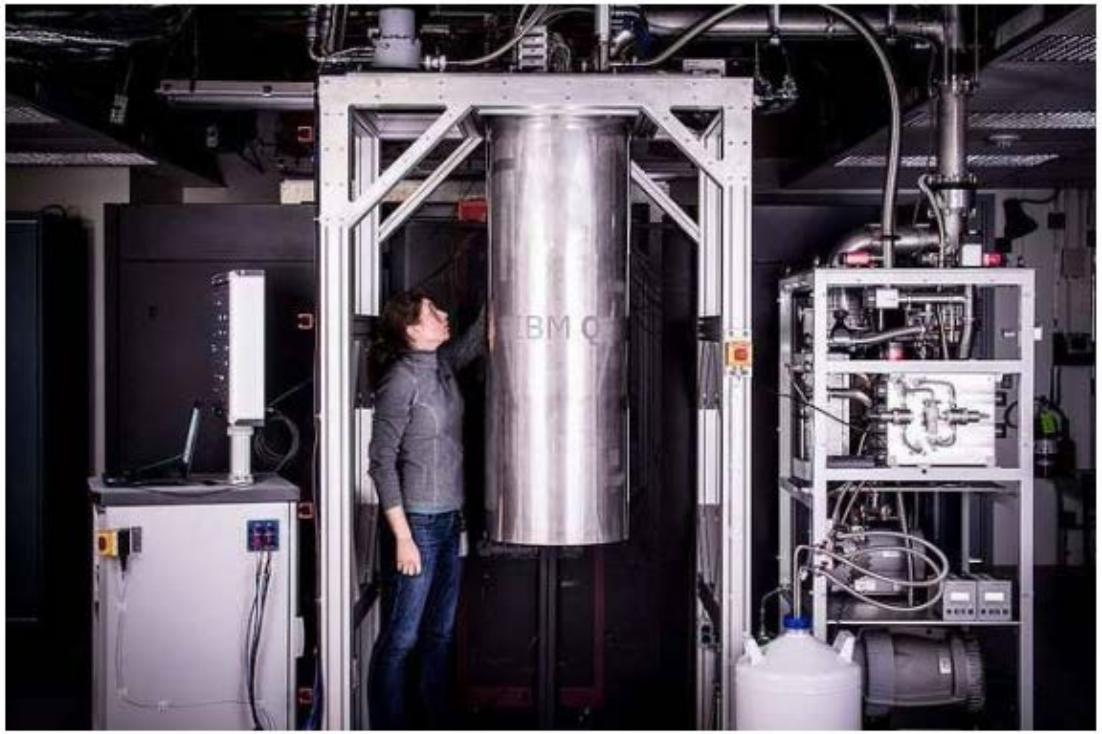
arXiv:1705.02435v1 [physics.app-ph] 6 May 2017



PHYS.ORG

IBM builds its most powerful universal quantum computing processors

May 17, 2017



nature COMMUNICATIONS

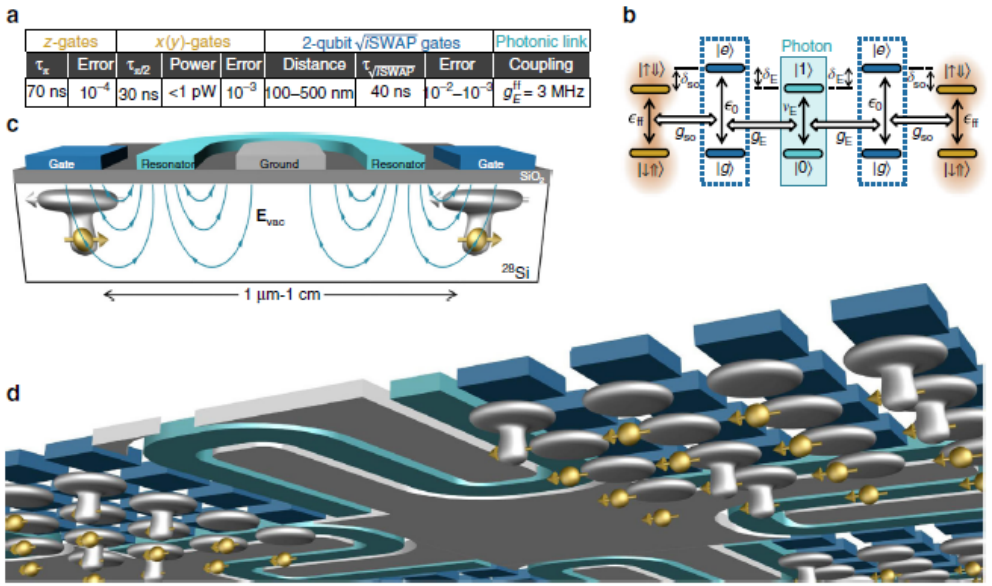
Published online: 06 September 2017

ARTICLE

DOI: 10.1038/s41467-017-00378-x OPEN

Silicon quantum processor with robust long-distance qubit couplings

Guilherme Tosi[1], Fahd A. Mohiyaddin[1,3], Vivien Schmitt[1], Stefanie Tenberg[1], Rajib Rahman[2], Gerhard Klimeck[2] & Andrea Morello[1]



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”

[London, September 2017]*: “1/6 chance within 10 years”*

S. Benjamin:
[London, September 2017]: *Speculates that if someone is willing to “go Manhattan project” then “maybe 6-12 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**

What is *y* (migration timeline)?

Quantum-safe cryptographic tool-chest

Conventional quantum-safe cryptography

a.k.a. Quantum Resistant Algorithms or Post-Quantum Cryptography

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

+

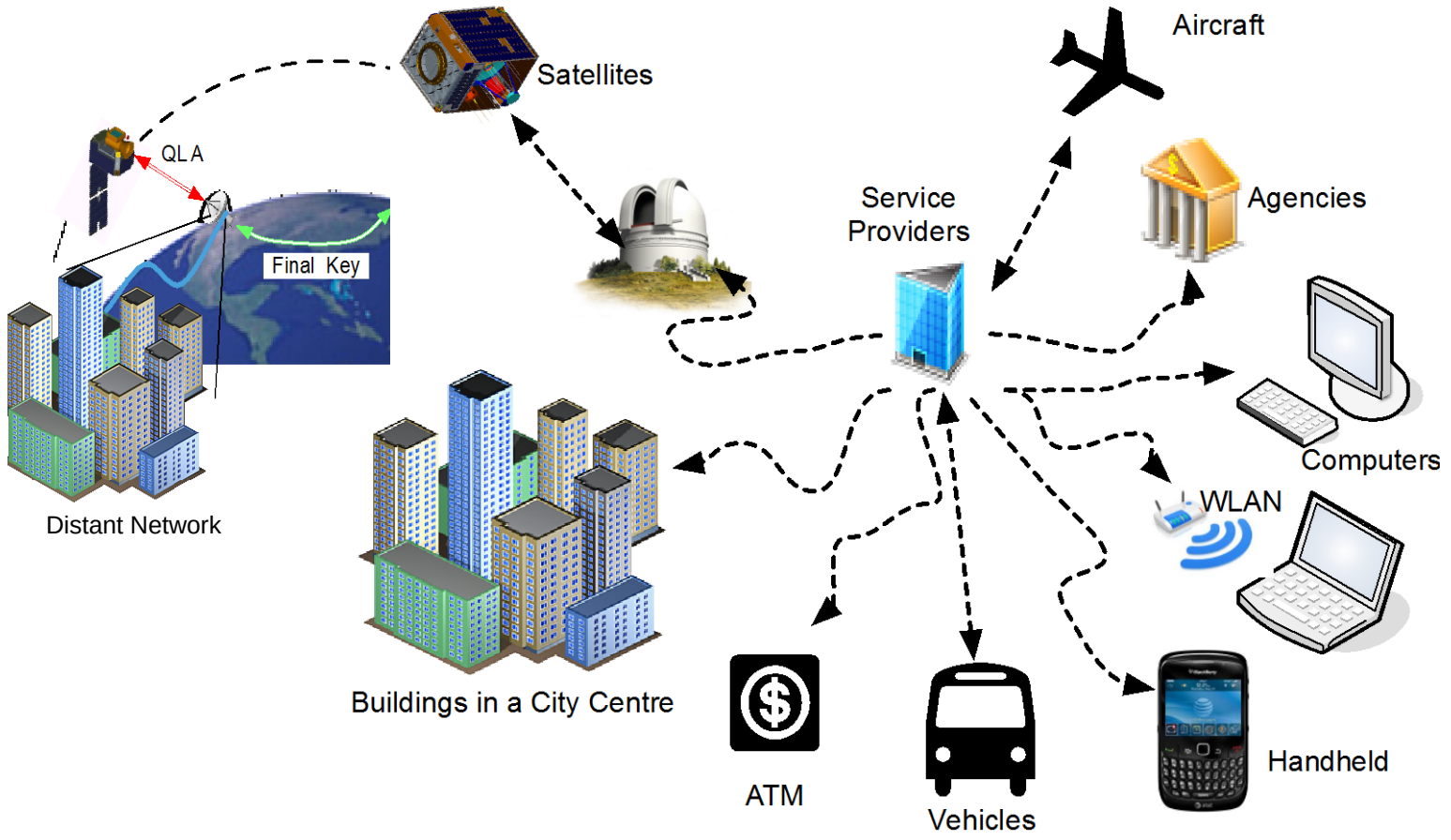
Quantum cryptography

- 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 Internet – The Long Term Vision

Qubit distribution with moving systems: satellites, aircraft, vehicles, ships, handheld



(Thanks to Thomas Jennewein)

Ongoing work to develop standards and certifications for these tools

- Are these algorithms actually secure against quantum attacks?
- Will these systems interoperate?
- Are the protocols implemented correctly?
- How can we be sure the quantum apparatus is behaving correctly?

e.g.

National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

ETSI / IQC Quantum Safe Workshop

13-15 SEPTEMBER 2017 ADD THIS TO MY CALENDAR

THERE IS NO CHARGE FOR THIS EVENT

WESTMINSTER CONFERENCE CENTRE, LONDON EXPAND

The 5th ETSI/IQC Workshop will take place in London (UK) on **13 – 15 September 2017**.
It will start with a special **Executive Track** on **13 September** and will be followed by an **in depth technical track** on **14-15 September 2017,** on which ETSI is currently **calling for presentations and poster session.**

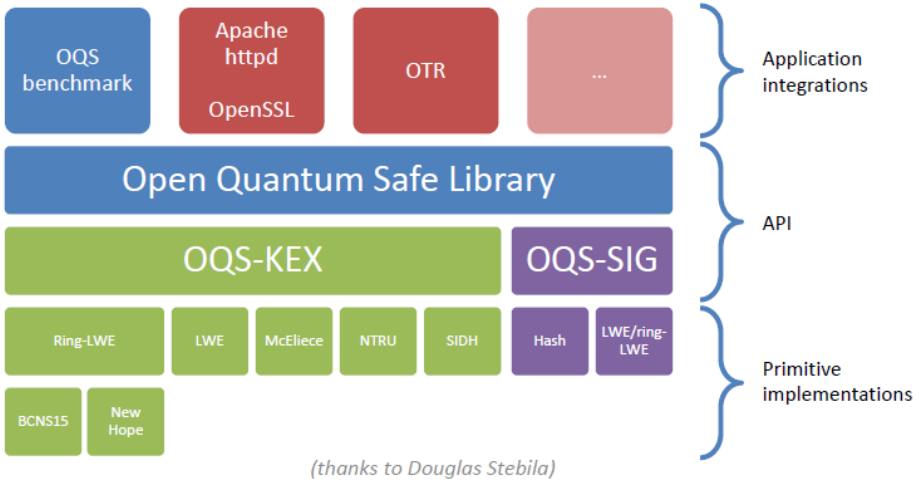
Partners

Terms of Reference for ETSI TC Cyber Working Group for Quantum-Safe Cryptography (ETSI TC Cyber WG-QSC)

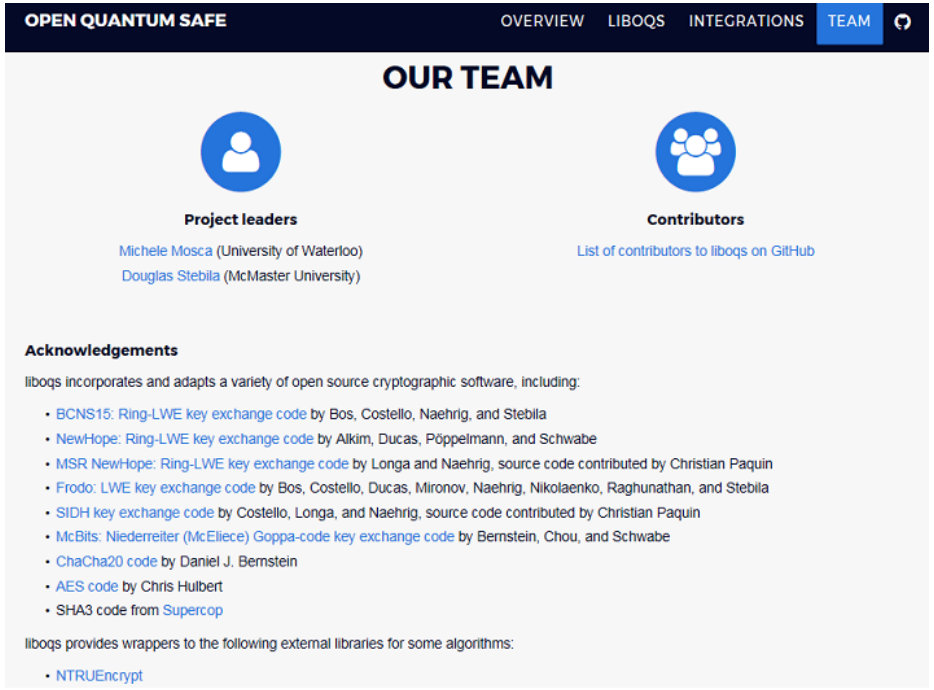
Approved at ETSI CYBER#09, 02/17

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

“But we’re risk-averse!”

Hybrid deployment of quantum-safe with currently deployed crypto provides strictly better security

Quantum Risk Fundamentals

Identify:

- Your organization’s reliance on cryptography
- The sources and types of technology in use

Track:

- The state of quantum technology development
- Advances in the development of quantum-safe technologies and algorithms

Manage:

- IT procurement to communicate the issue to vendors
- Technology upgrades and lifecycles to facilitate the incorporation of quantum-safe algorithms

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

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”

Security is a choice

Does your organization have a plan?

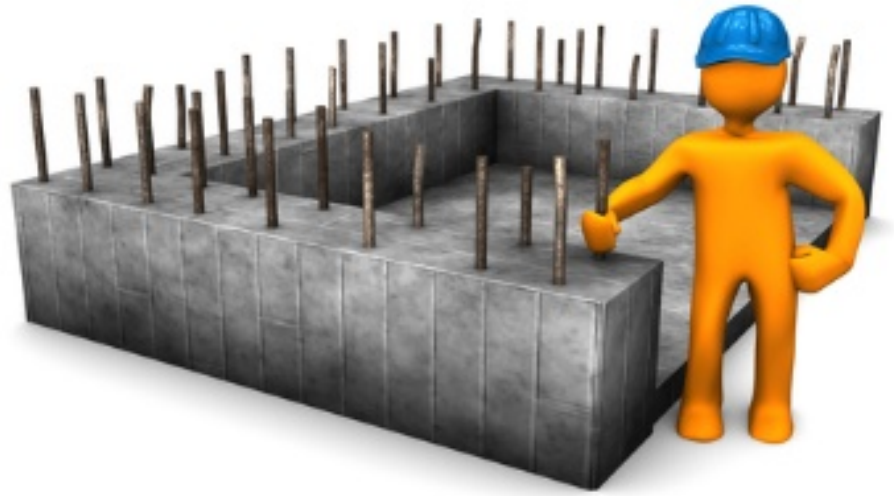
Who is responsible for it?

Do your vendors have a plan?

Does your industry have plan?

Are these plans coordinated?

Historic opportunity



Thank you!

Comments, questions and feedback are very welcome

Michele Mosca
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
CEO, evolutionQ Inc.
michele.mosca@evolutionq.com

Questions