The quantum threat: What really matters today?

Vlad Gheorghiu &
Michele Mosca

15 November 2017
SecTor Toronto

CryptoWorks21

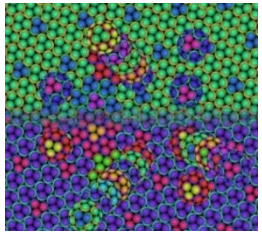
PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

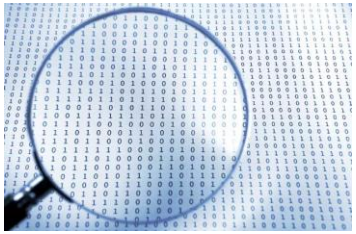
evolution

Quantum-Safe CANADA

Quantum paradigm brings new possibilities



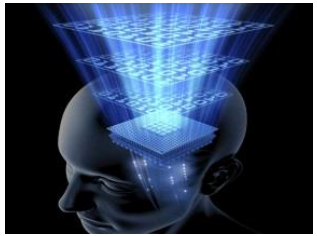
Designing new materials, drugs, etc.



Optimizing

Sensing and measuring

Secure communication



What else???

But… while in the old paradigm

3967241
x 5289737

20985661505617

Encrypting is EASY

50668036014097494832 3
= ??????????????? x
???????????????

Codebreaking is HARD!

…in the quantum paradigm

3967241
x 5289737

20985661505617

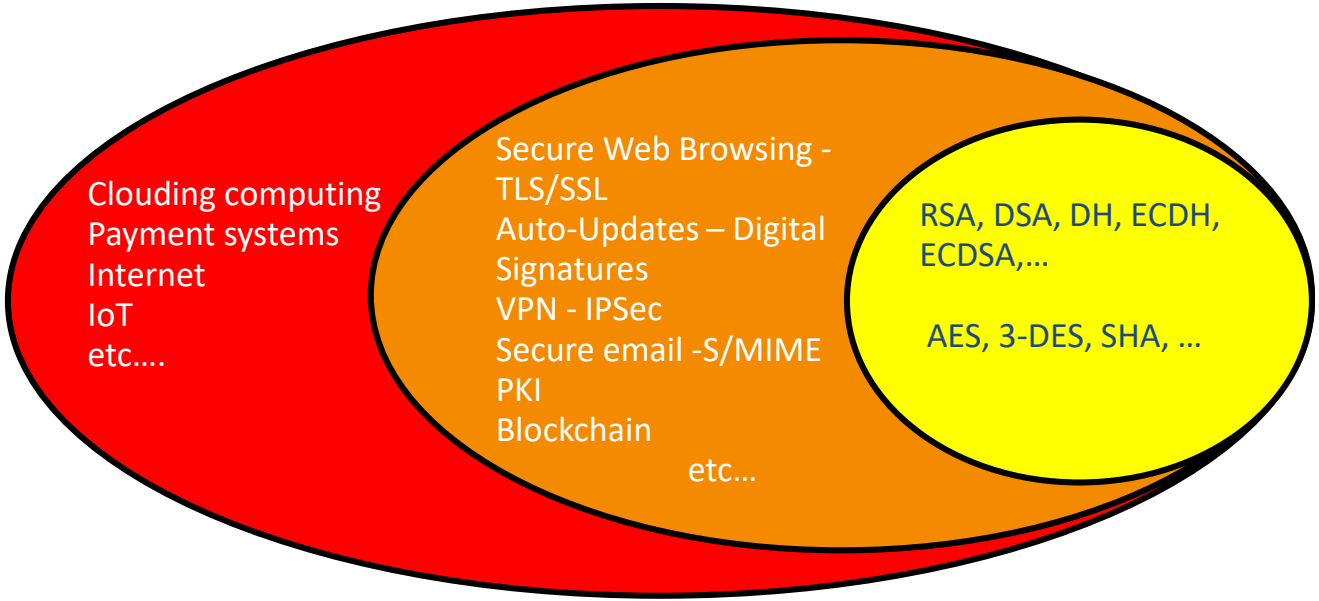
Encrypting is EASY

50668036014097494832 3
= 13561998077
x 37360303199

Codebreaking is EASY!

What will be affected?

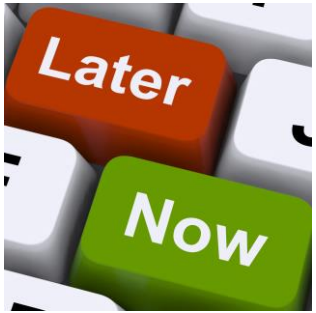
Products, services, business functions that rely on security products will either stop functioning or not provide the expected levels of security.



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.

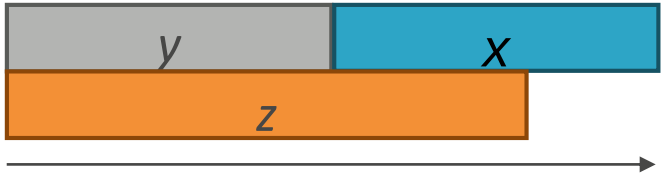
Do we need to worry *now*?



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.

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*]

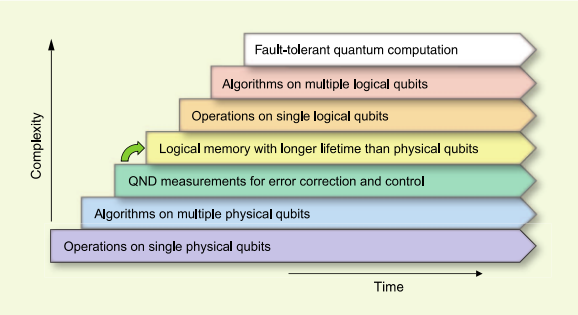


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third 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?

SCIENCE TECH DIY GOODS VIDEO ROLL THE DICE SUBSCRIBE

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

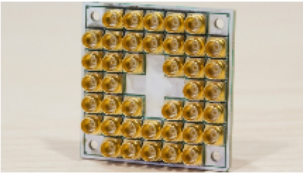
The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.

Intel brings Quantum computing a step closer to reality

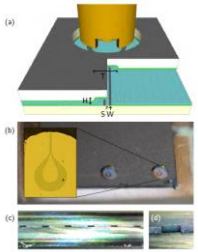
BY ROHITH BHASKAR OCT. 12, 2017, 2:57 P.M.

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



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 Industries & solutions Services Products Support & downloads My IBM

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

News room > News releases >

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

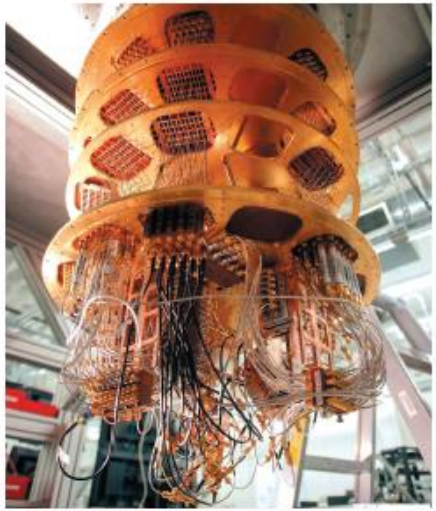
News release | Contact(s) information
Related XML feeds | Related resources

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.

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?



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.

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

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”*

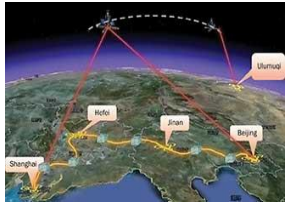
Quantum-safe cryptographic tool-chest

conventional quantum-safe cryptography

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

+

quantum cryptography



Courtesy of Qiang Zhang, USTC

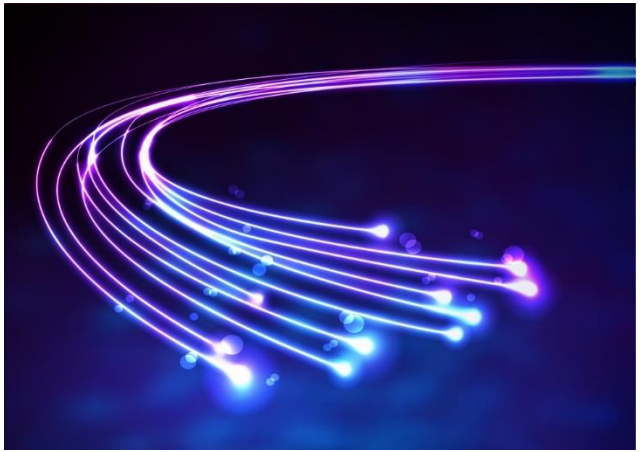
http://www.idquantique.com/photon-counting/clavis3-qkd-platform/

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

Quantum cryptography

For this talk, focus on key establishment –

"Quantum key distribution" (QKD):



Quantum physics guarantees the cryptographic security of the key

Over time, QKD evolves from:

Point-to-Point

→

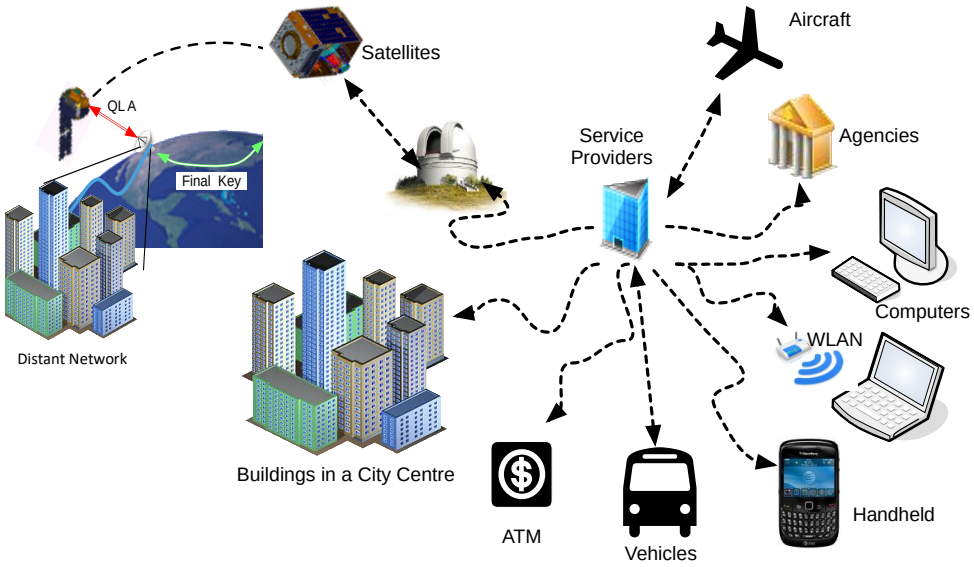
Trusted Repeater Networks

→

Untrusted Repeater Networks

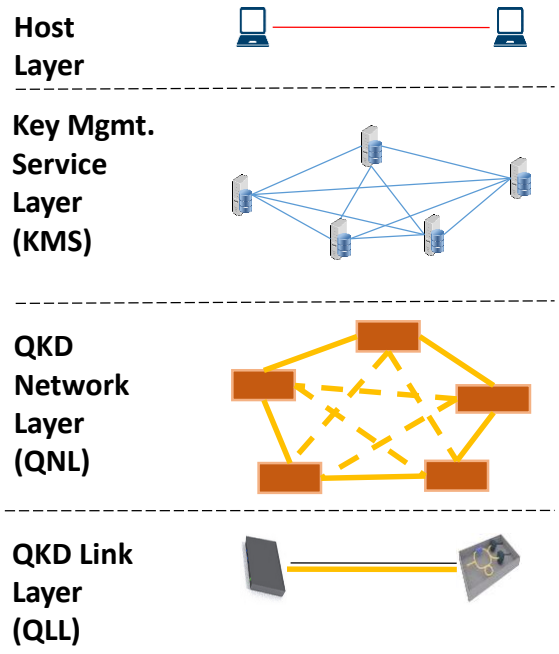
Quantum Internet – the Long Term Vision

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



(Thanks to Thomas Jennewein)

Protocol stack for QKD



Can *design* QKD into systems *today* as a key establishment alternative.

Global thought leadership in Canada

Academic research (post-quantum, QKD, quantum crypto beyond QKD)

Standards

- Founding member of ETSI QKD ISG
- Creation of ETSI QSC ISG
- participation in NIST Post-Quantum Process

Quantum-Safe Awareness

- spreading the gospel of quantum-safe cryptography
- ETSI White Paper on quantum-safe cryptography

Implementation

- Training of Workforce (CryptoWorks21)
- Technology Transfer
  - Open Quantum Safe Project (openquantumsafe.org)
  - Spin-off companies

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”

“But we’re risk-averse!”

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

Quantum Risk Fundamentals

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

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.

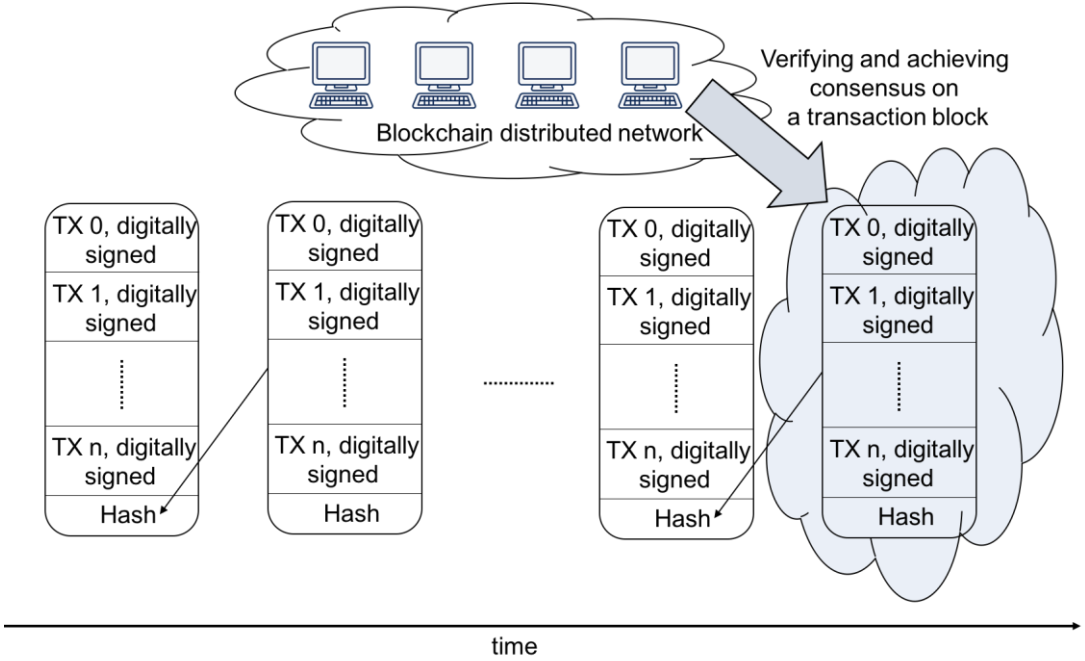
Security is a choice

Does your organization have plan?
Who is responsible for it?
Do your vendors have a plan?

Does your industry have plan?
Are these plans coordinated?

Historic opportunity

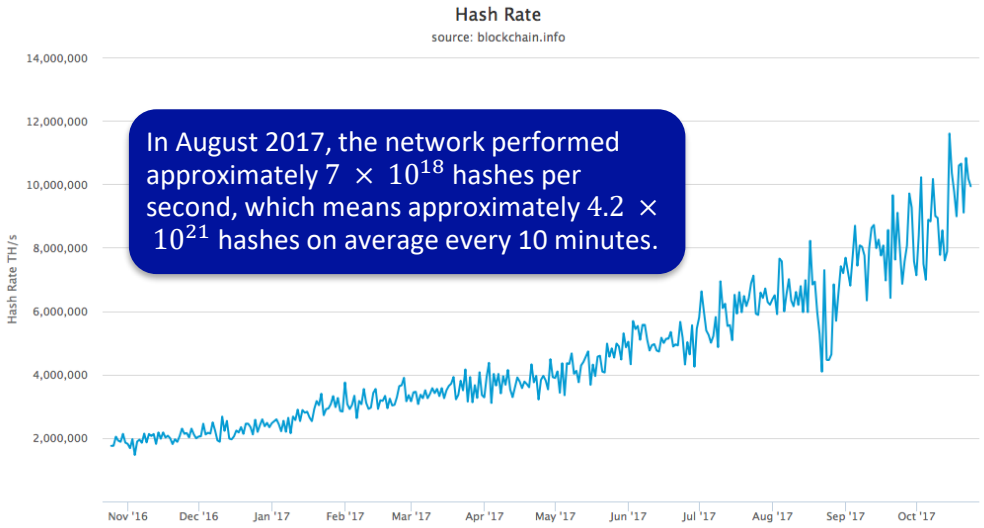
Concrete example: Blockchains



- Distributed ledger of trust
- Trust is achieved via a collective consensus mechanism
- Immutable
- Time-stamping service

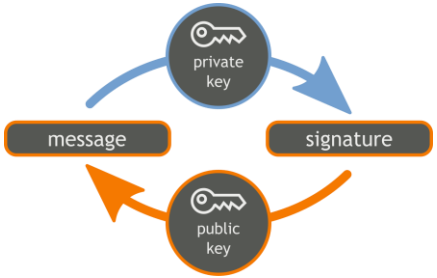
Work based on

- Various **consensus mechanisms**: proof of work ("hard" mathematical puzzles) - Bitcoin, proof of stake (Byzantine-agreement-like protocols) - future fork of Ethereum etc. Weakened by quantum computers (not broken).



In August 2017, the network performed approximately 7×10^{18} hashes per second, which means approximately 4.2×10^{21} hashes on average every 10 minutes.

- Authentication is achieved via **digital signatures** (EC-DSA etc)**.**
- **100% VULNERABLE!**



Work based on

Towards quantum-resistant Blockchains

- Authentication (digital signature) – **CATASTROPHIC**
- Consensus mechanism (hash functions, Byzantine agreement etc.) – **WEAKENED**, **NOT BROKEN**
- Two "problems" to tackle:
  1. Patching (making quantum-safe) existing Blockchains (harder)
  2. Building quantum-safe Blockchains from scratch (easier)

Work based on

Patching existing Blockchains

- Current Blockchains are not quantum-safe (e.g. Bitcoin)

- Need to patch at least the authentication part.
  - E.g., at a given time in the future, be able to change the digital signature with a quantum-resistant one, and “force” all users to perform a transaction in which assets are transferred to a new quantum-resistant wallet

- Consensus mechanism seems ok (at least in the near future)
  - Worst case scenario: asymmetric quantum adversary
  - Highly unlikely
  - 1st gen. of quantum computers: need 30’000 in parallel to crack the PoW

Work based on

Work based on

Designing quantum-resistant Blockchains from scratch

- Simpler: use only quantum-resistant cryptographic (post-quantum) schemes
- **Main issue: scalability/performance**

Post-quantum scheme	Public-key size	Private-key size	Signature size
Hash-based	1,056	1,088	41,000
Code-based	192,192	1,400,288	370
Lattice-based	7,168	2,048	5,120
Ring-LWE-based	7,168	4,608	3,488
Multivariate-based	99,100	74,000	424
Isogeny-based	768	48	141,312
Isogeny-based (compressed)	336	48	122,880

- In comparison, a current EC-DSA signature is only 71 bytes long!

Other challenges

- Lack of established post-quantum standards. In progress (NIST, ETSI)
- More research in post-quantum schemes
- What can we do NOW?
  - Be crypto-agile and software-agile!
  - Build prototypes with existing post-quantum systems.
  - Test and improve
  - Keep an eye on advances in fault-tolerant quantum computing, and post-quantum development.
  - Use competent developers who (**really**) understand how to implement cryptography securely!

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.

INTERNATIONAL CRYPTOGRAPHIC MODULE CONFERENCE 2017

May 16-19 | Westin Arlington Gateway | Washington, DC

Special-Focus Conference Content

Following suggestions from the survey responses of previous attendees and the guidance of our industry expert program committee, the conference features content in six key areas:

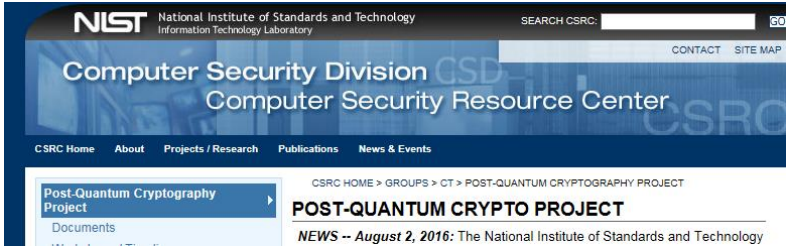
Global Cryptographic Module Validation: ICMC will continue its strong focus on North American validation programs and we've added a half day on global validation with reports from various international verification bodies, and prospects for an international validation (iCMVP) scheme. More info.

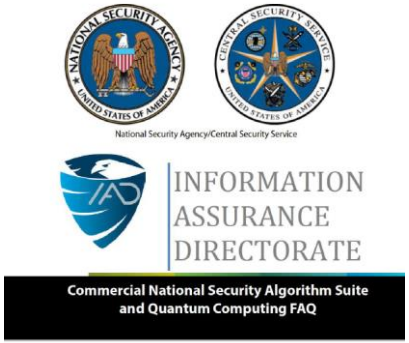
Open Source Cryptography: OpenSSL is the most widely used encryption software library in the world, but last year saw threats to its security and future certification. We'll cover efforts to audit and improve the security of OS encryption. More info.

Common Criteria: The crypto certification community is widely involved in Common Criteria, so ICMC provides a great opportunity for discussions on the prospect for CC in Crypto, and efforts to bring CC to broader user base. More info.

Quantum Threats and Quantum-Safe Crypto: Many approved algorithms can be easily broken by theoretical quantum computers. We've scheduled a day's worth of content focused on this emerging threat, as well as the transition to standardized quantum-safe algorithms. More info.

Ongoing work to develop standards and certifications for these tools





What to expect next?

NIST will post "complete and proper" submissions for security and performance analysis at www.nist.gov/pqcrypto , that is,

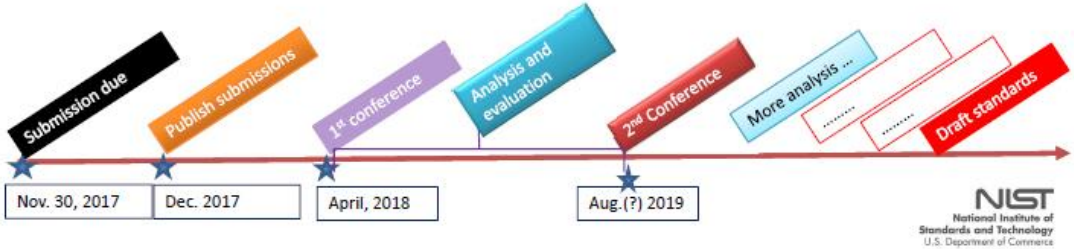
- The submitted candidates are publicly available for scrutinizing and evaluating

The First NIST PQC Standardization Conference (co-located with PQCrypto, April 2018)

- For submitters to present the algorithms and design rationale
- For researchers and practitioners to ask questions on the submitted algorithms

Evaluation and analysis continue after The First NIST PQC Standardization Conference (~16 months)

The Second NIST PQC Standardization Conference is planning to be held in the second half of 2019 (tentative Aug. 2018 to be confirmed)

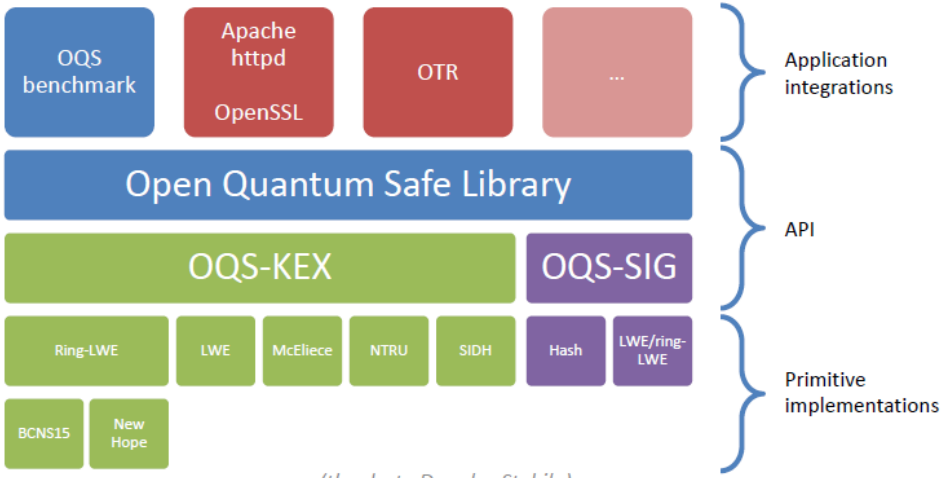


(by Lily Chen: https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S03_THREATS/NIST_CHEN.pdf)

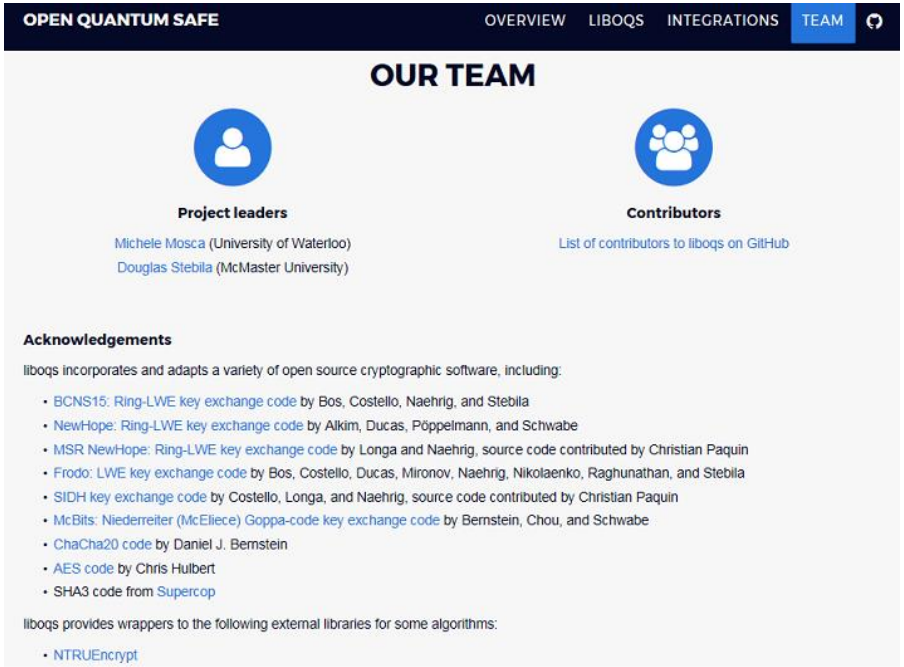
openquantumsafe.org

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

- Open source, runs on UNIX/Linux/Windows/ARM etc.
- Collaborative effort. Project leaders: Michele Mosca (University of Waterloo), Douglas Stebila (McMaster University).
- Prototype post-quantum cryptography in protocols and applications
- Incorporates and adapts a variety of open source cryptographic software
- Testing new algorithms (allows algorithm switching both at compile-time and run-time)
- Benchmarking suite, continuous integration
- Long term goal: support the development and prototyping of quantum-resistant cryptography (NIST submissions etc.)

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

Co-Founder and CEO evolutionQ Inc.
www.evolutionq.com
michele.mosca@evolutionq.com

Vlad Gheorghiu

Post-doctoral fellow,
Institute for Quantum Computing

Quantum Risk Researcher
evolutionQ Inc. www.evolutionq.com

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

Homework?