The quantum threat: What really matters today?

Vlad Gheorghiu & Michele Mosca

15 November 2017
SecTor Toronto
Quantum paradigm brings new possibilities

Designing new materials, drugs, etc.
Optimizing
Sensing and measuring
Secure communication
What else???

©Michele Mosca & Vlad Gheorghiu
But... while in the old paradigm

Encrypting is **EASY**

Codebreaking is **HARD!**

©Michele Mosca & Vlad Gheorghiu
...in the quantum paradigm

Encrypting is EASY

3967241
x 5289737
20985661505617

506680360140974948323
= 13561998077
x 37360303199

Codebreaking is EASY!

©Michele Mosca & Vlad Gheorghiu
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.

Clouding computing
Payment systems
Internet
IoT
etc....

Secure Web Browsing - TLS/SSL
Auto-Updates – Digital Signatures
VPN - IPSec
Secure email - S/MIME
PKI
Blockchain
etc...

RSA, DSA, DH, ECDH, ECDSA, ...

AES, 3-DES, SHA, ...

©Michele Mosca & Vlad Gheorghiu
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.


©Michele Mosca & Vlad Gheorghiu
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.

©Michele Mosca & Vlad Gheorghiu
How close are we to having sufficient quantum resources?

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.
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.

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.


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.”

©Michele Mosca & Vlad Gheorghiu
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

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

©Michele Mosca & Vlad Gheorghiu
Quantum cryptography

For this talk, focus on key establishment – “Quantum key distribution” (QKD):

Over time, QKD evolves from:
- Point-to-Point
- Trusted Repeater Networks
- Untrusted Repeater Networks

Quantum physics guarantees the cryptographic security of the key
Quantum Internet – the Long Term Vision

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

Distant Network
Buildings in a City Centre
Satellites
Aircraft
Vehicles
Service Providers
Agencies
Computers
Handheld
WLAN

Final Key

©Michele Mosca & Vlad Gheorghiu

(Thanks to Thomas Jennewein)
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

©Michele Mosca & Vlad Gheorghiu
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

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 a plan? Does your industry have a plan? Who is responsible for it? Are these plans coordinated? Do your vendors have a plan?
Historic opportunity
Concrete example: Blockchains

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

Work based on

©Michele Mosca & Vlad Gheorghiu
• 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).

• Authentication is achieved via **digital signatures** (EC-DSA etc).

• **100% VULNERABLE!**

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

Work based on [Quantum Safe Blockchains](https://www.blockchainresearchinstitute.org)
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
Designing quantum-resistant Blockchains from scratch

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

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

- 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!
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?

Ongoing work to develop standards and certifications for these tools.

©Michele Mosca & Vlad Gheorghiu
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)
Testing new tools

openquantumsafe.org

Open Quantum Safe Library

OQS benchmark
Apache httpd
OpenSSL
OTR
...

OQS-KEX
OQS-SIG

Ring-LWE
LWE
McEliece
NTRU
SIDH
Hash
LWE/ring-LWE

API

Application Integrations

Primitive Implementations

(thanks to Douglas Stebila)

©Michele Mosca & Vlad Gheorghiu
• 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/~mmasca
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?

©Michele Mosca & Vlad Gheorghiu