SECURE TECHNOLOGY ALLIANCE

utimaco®

The Latest View on Quantum Computing and its Impact on Critical Digital Infrastructures

9 December 2020

Michele Mosca

evolutionQ

PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

softwareQ

Quantum-Safe CANADA

CYBER SECURITY AND PRIVACY INSTITUTE
UNIVERSITY OF WATERLOO

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

QUANTUM INDUSTRY CANADA

Are you quantum-ready?

- Do you understand what the technologies are capable of and their readiness levels?

- Do you understand how the new capabilities impact your organization or sector?

- Do you have a plan to benefit from the disruptive capabilities?

- Do you have a plan to mitigate any quantum threats?

Cloud computing, payment systems, internet, IoT, eHealth, etc…

Secure web browsing, Auto-updates, VPN, Secure email, Blockchain, etc…

Cryptography:RSA, [illegible] DH, ECDH, ECDSA,…, SHA, AES

3 inflection points

- NIST standards (2022-24): will you be 75% ready by then?

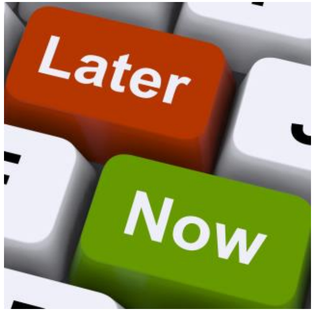
- Fault-tolerant logical qubit: will you be 90% ready by then?
- Commercial long-distance QKD: will you be QKD-ready?

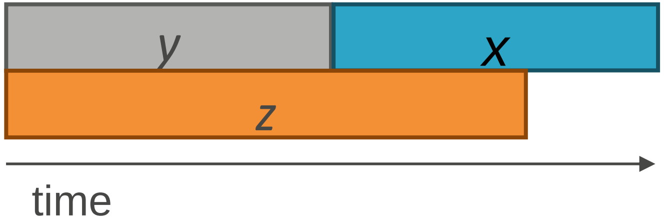
Do we need to worry *now*?

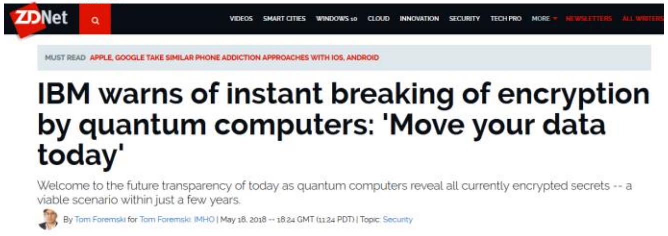
Depends on*:

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

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







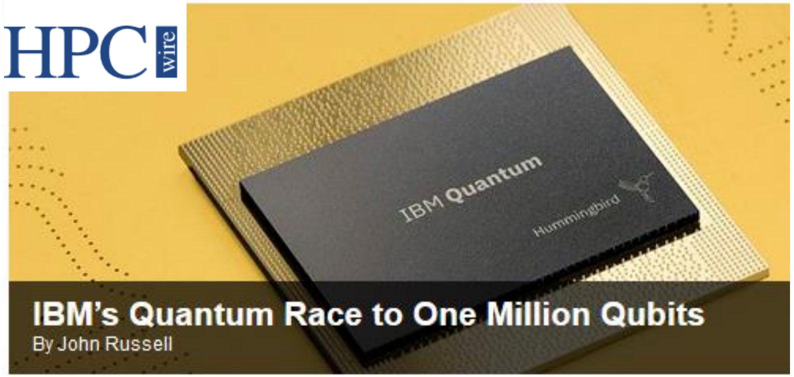
MUST READ APPLE, GOOGLE TAKE SIMILAR PHONE ADDICTION APPROACHES WITH IOS, ANDROID

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.

By Tom Foremski for Tom Foremski: IMHO | May 18, 2018 -- 18:24 GMT (11:24 PDT) | Topic: Security

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

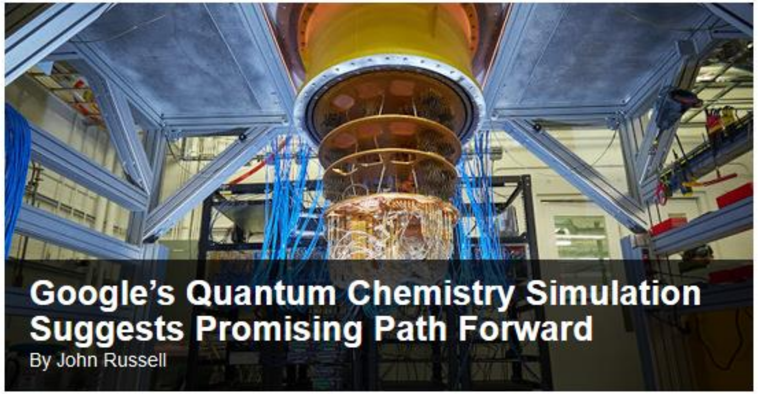


IBM's Quantum Race to One Million Qubits

By John Russell

September 15, 2020

Hummingbird (65 qubits).

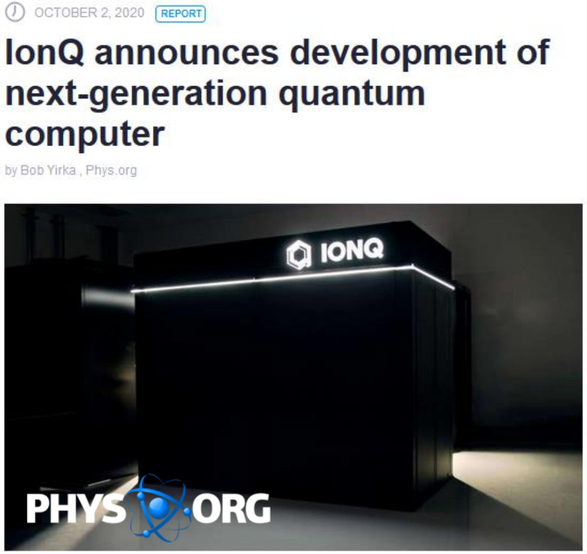


Google's Quantum Chemistry Simulation Suggests Promising Path Forward

By John Russell

HPC wire

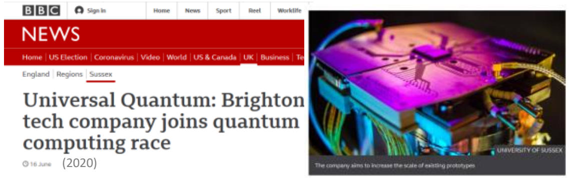
September 9, 2020



OCTOBER 2, 2020 REPORT

IonQ announces development of next-generation quantum computer

by Bob Yirka , Phys.org



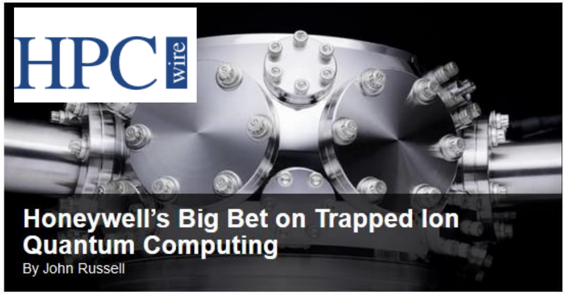
Home | News | Sport | Reel | Worklife

Home | US Election | Coronavirus | Video | World | US & Canada | UK | Business | Te
England | Regions | Sussex

Universal Quantum: Brighton tech company joins quantum computing race

16 June (2020)

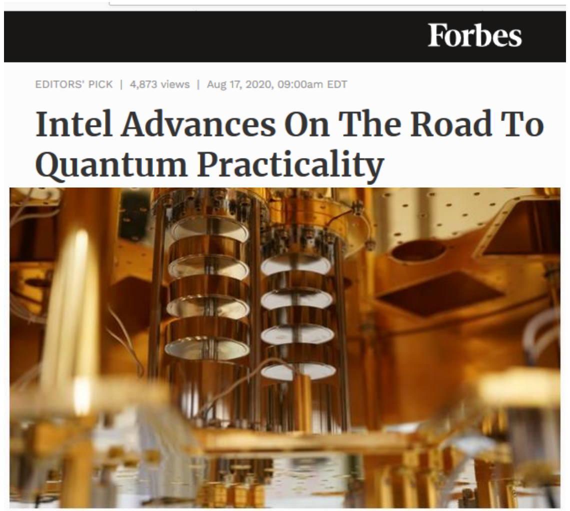
The company aims to increase the scale of existing prototypes



Honeywell's Big Bet on Trapped Ion Quantum Computing

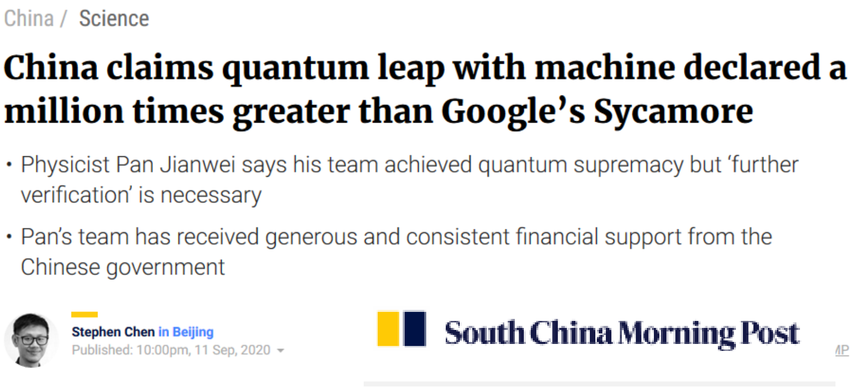
By John Russell

April 7, 2020



EDITORS' PICK | 4,873 views | Aug 17, 2020, 09:00am EDT

Intel Advances On The Road To Quantum Practicality



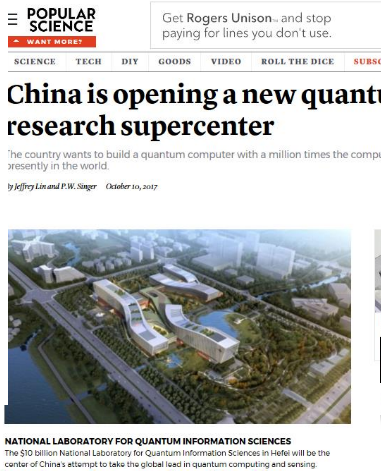
China / Science

China claims quantum leap with machine declared a million times greater than Google's Sycamore

- Physicist Pan Jianwei says his team achieved quantum supremacy but 'further verification' is necessary
- Pan's team has received generous and consistent financial support from the Chinese government

Stephen Chen in Beijing
Published: 10:00pm, 11 Sep, 2020

South China Morning Post



POPULAR SCIENCE
WANT MORE?

SCIENCE | TECH | DIY | GOODS | VIDEO | ROLL THE DICE | SUBSCRIBE

China is opening a new quantum research supercenter

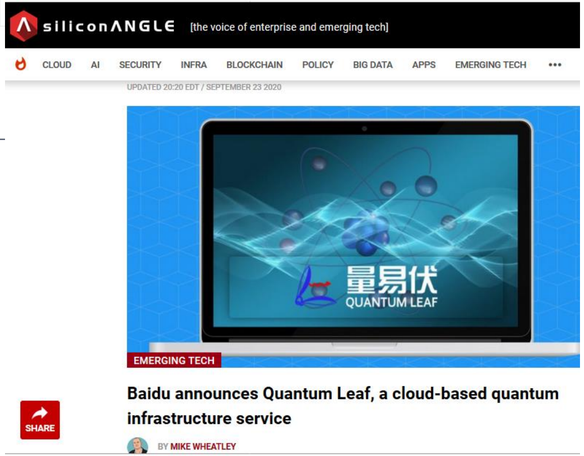
The country wants to build a quantum computer with a million times the computing power presently in the world.

By Jeffrey Lin and P.W. Singer October 10, 2017

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



siliconANGLE [the voice of enterprise and emerging tech]

CLOUD | AI | SECURITY | INFRA | BLOCKCHAIN | POLICY | BIG DATA | APPS | EMERGING TECH

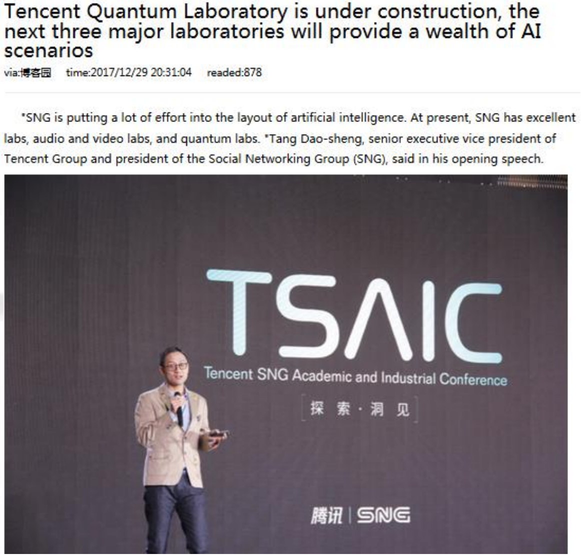
UPDATED 20:20 EDT / SEPTEMBER 23 2020

EMERGING TECH

Baidu announces Quantum Leaf, a cloud-based quantum infrastructure service

SHARE

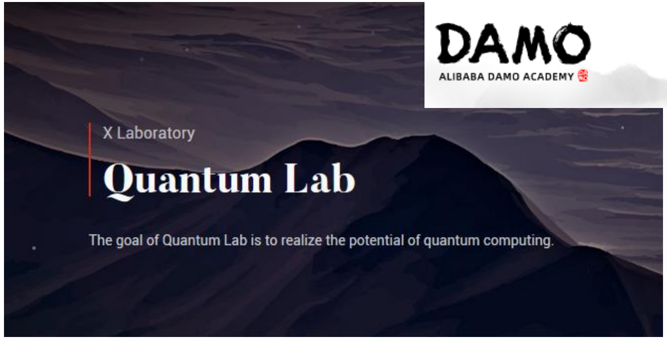
BY MIKE WHEATLEY



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

via:博客园 time:2017/12/29 20:31:04 readed:878

"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-sheng, senior executive vice president of Tencent Group and president of the Social Networking Group (SNG), said in his opening speech.

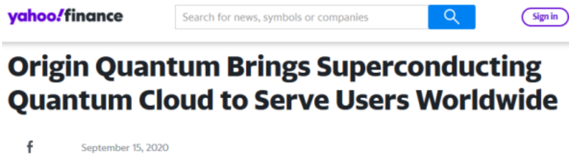


DAMO
ALIBABA DAMO ACADEMY

X Laboratory

Quantum Lab

The goal of Quantum Lab is to realize the potential of quantum computing.

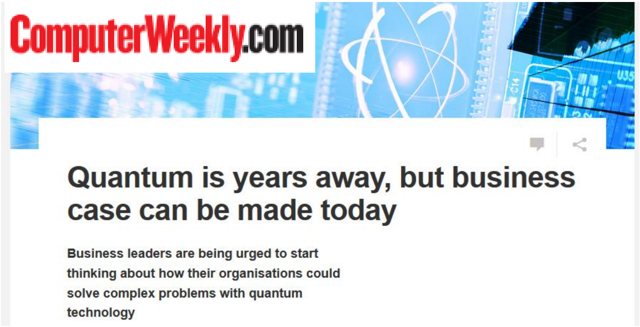


yahoo!finance

Search for news, symbols or companies | Sign in

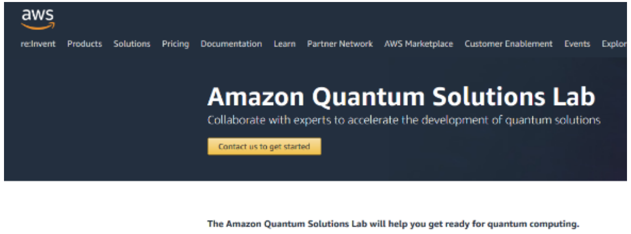
Origin Quantum Brings Superconducting Quantum Cloud to Serve Users Worldwide

September 15, 2020


ComputerWeekly.com

Quantum is years away, but business case can be made today

Business leaders are being urged to start thinking about how their organisations could solve complex problems with quantum technology

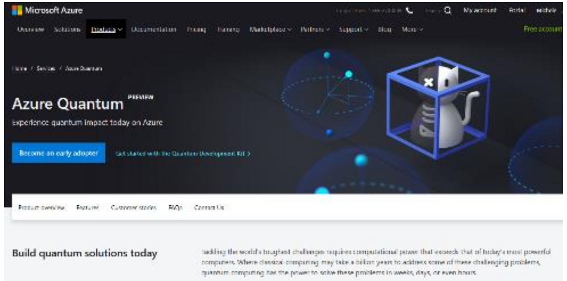

aws
re:Invent Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explor

Amazon Quantum Solutions Lab

Collaborate with experts to accelerate the development of quantum solutions

Contact us to get started

The Amazon Quantum Solutions Lab will help you get ready for quantum computing.


Microsoft Azure
My account Portal
Overview Solutions Products Documentation Pricing Training Marketplace Partners Support Blog More
Free account
Home / Services / Azure Quantum

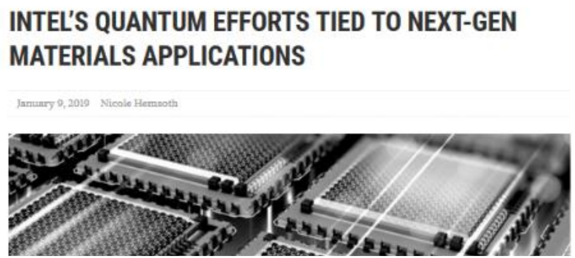
Azure Quantum PREVIEW

Experience quantum impact today on Azure

Become an early adopter
Get started with the Quantum Development Kit >
Product overview Features Customer stories FAQs Contact Us

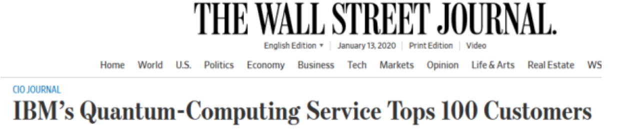
Build quantum solutions today

Tackling the world's toughest challenges requires computational power that exceeds that of today's most powerful computers. Where classical computing may take a billion years to address some of these challenging problems, quantum computing has the power to solve these problems in weeks, days, or even hours.



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

January 9, 2019 Nicole Hemsoth


THE WALL STREET JOURNAL.

English Edition ▾ | January 13, 2020 | Print Edition | Video
Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WS

CIO JOURNAL

IBM's Quantum-Computing Service Tops 100 Customers

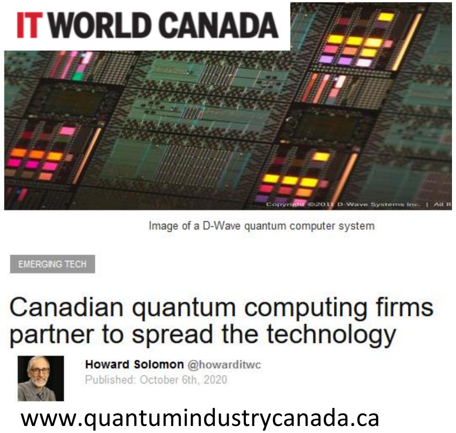

IT WORLD CANADA

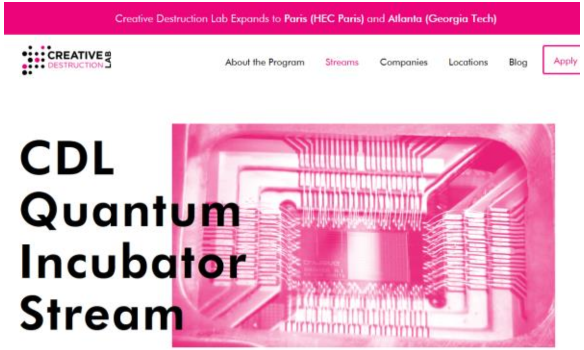
Image of a D-Wave quantum computer system

EMERGING TECH

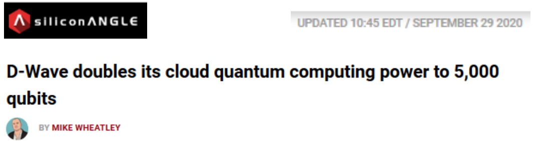
Canadian quantum computing firms partner to spread the technology

Howard Solomon @howarditwc
Published: October 6th, 2020

www.quantumindustrycanada.ca


Creative Destruction Lab Expands to Paris (HEC Paris) and Atlanta (Georgia Tech)

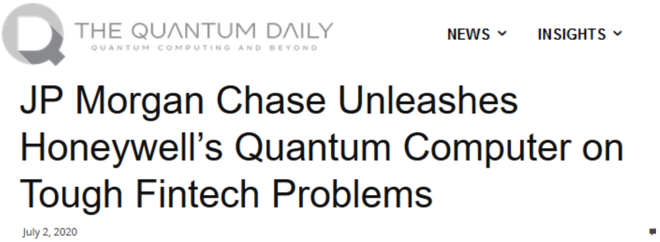
CDL Quantum Incubator Stream


siliconANGLE

UPDATED 10:45 EDT / SEPTEMBER 29 2020

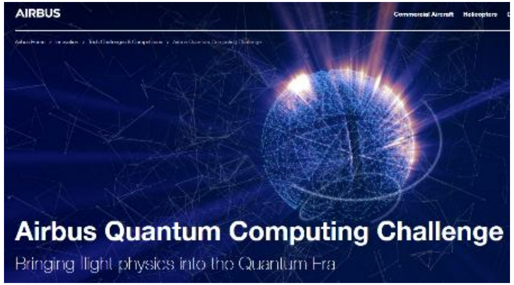
D-Wave doubles its cloud quantum computing power to 5,000 qubits

BY MIKE WHEATLEY


THE QUANTUM DAILY
QUANTUM COMPUTING AND BEYOND

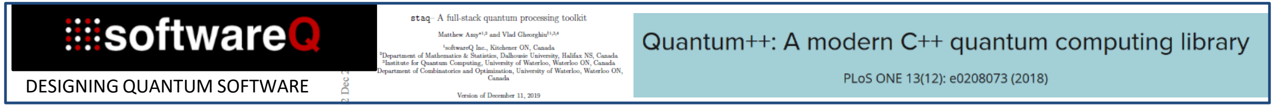
JP Morgan Chase Unleashes Honeywell's Quantum Computer on Tough Fintech Problems

July 2, 2020



Airbus Quantum Computing Challenge

Bringing flight physics into the Quantum Era


softwareQ

DESIGNING QUANTUM SOFTWARE

staq– A full-stack quantum processing toolkit

Matthew Amy*[1,2] and Vlad Gheorghiu†[1,3,4]

[1]softwareQ Inc., Kitchener ON, Canada
[2]Department of Mathematics & Statistics, Dalhousie University, Halifax NS, Canada
[3]Institute for Quantum Computing, University of Waterloo, Waterloo ON, Canada
Department of Combinatorics and Optimization, University of Waterloo, Waterloo ON, Canada

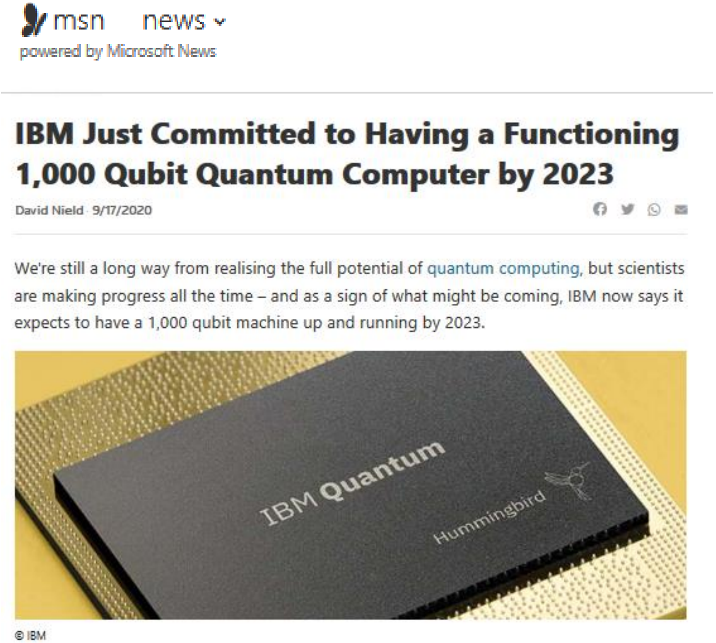
Version of December 11, 2019

12 Dec 2

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

PLoS ONE 13(12): e0208073 (2018)

Toward fault-tolerant logical qubits



IBM Just Committed to Having a Functioning 1,000 Qubit Quantum Computer by 2023

David Nield · 9/17/2020

We're still a long way from realising the full potential of quantum computing, but scientists are making progress all the time – and as a sign of what might be coming, IBM now says it expects to have a 1,000 qubit machine up and running by 2023.

© IBM

"…it would be enough to maintain a small number of stable, logical qubit systems that could then interact with each other."

IonQ says its record-breaking quantum computer is most powerful ever

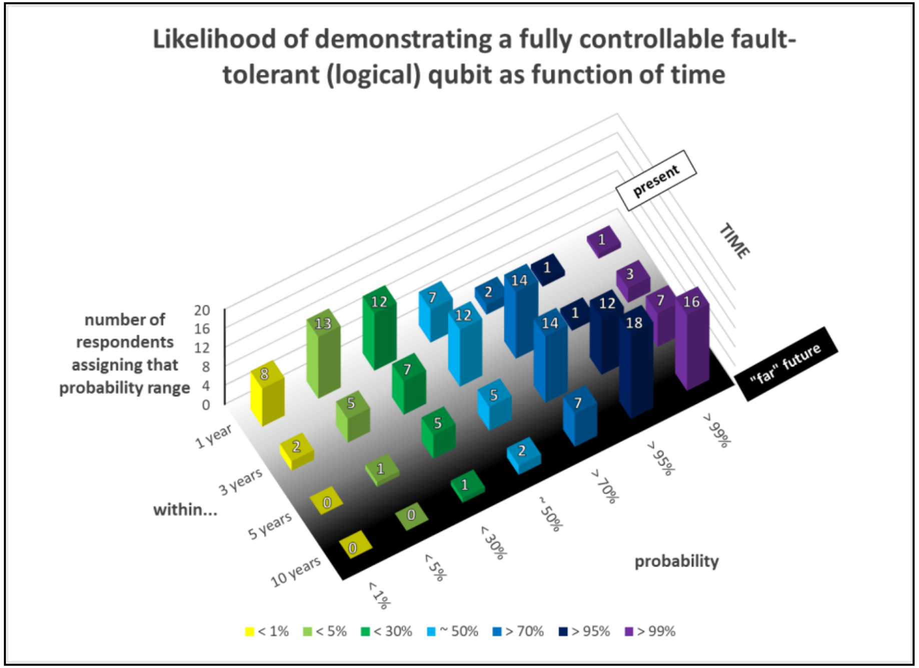
TECHNOLOGY 1 October 2020

By Leah Crane

The ion trap at the heart of IonQ's quantum computer

Kai Hudek, IonQ

When??



(In upcoming 2020 version of https://globalriskinstitute.org/publications/quantum-threat-timeline/.)

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**”.*

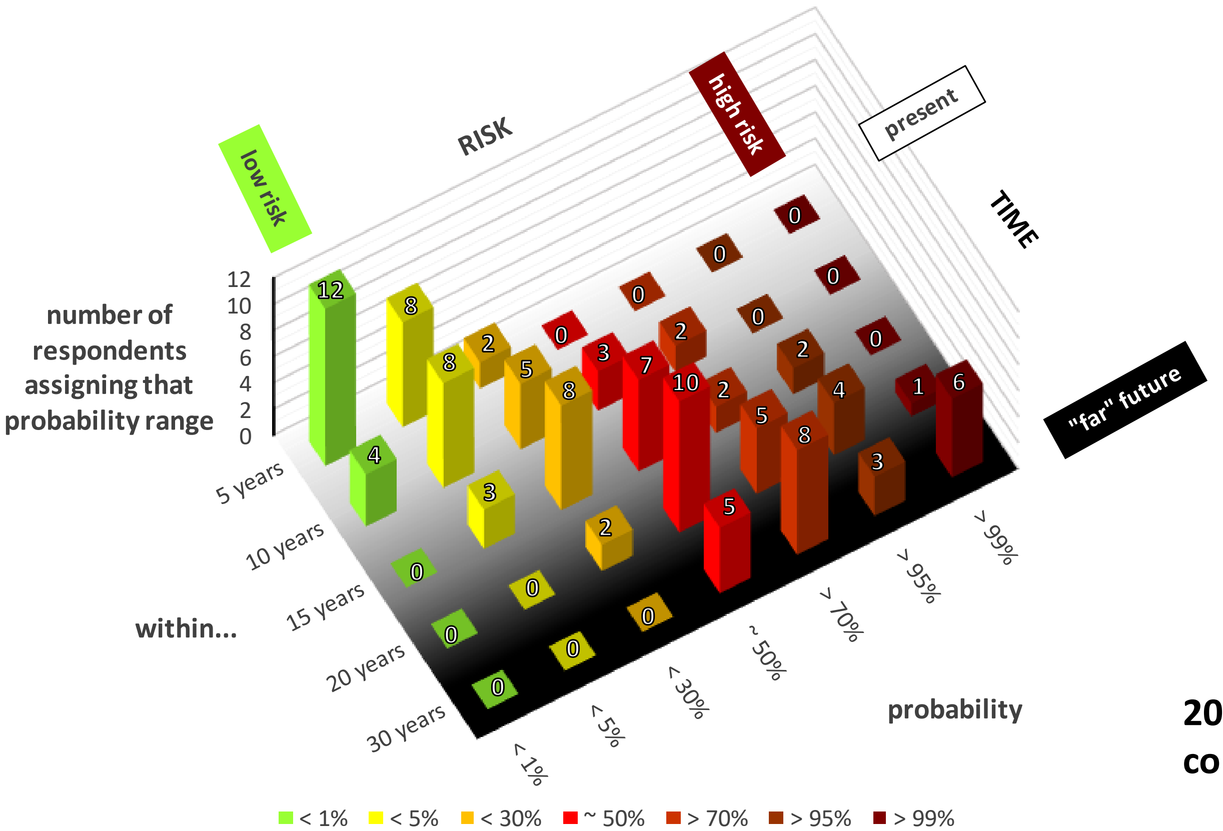
- **Michele Mosca** ([NIST, April 2015], [ISACA**,** September 2015]): *“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”*

- **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***

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



2020 New report coming out soon.

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

Quantum-safe cryptography tool-chest

conventional quantum-safe cryptography

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

+

quantum cryptography

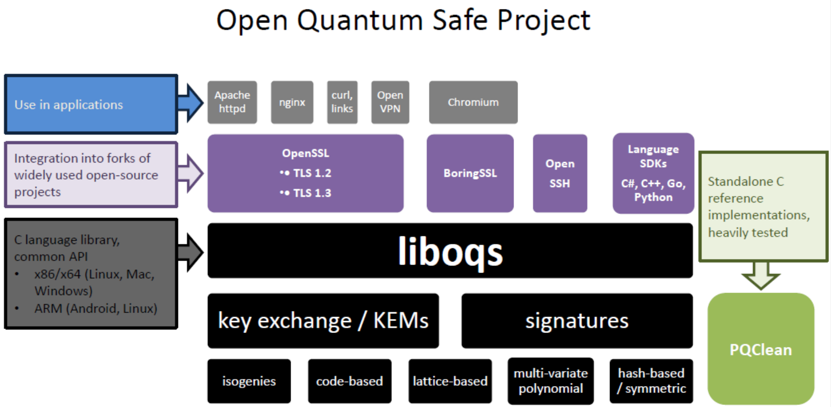
Courtesy of Qiang Zhang, USTC

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-safe" = designed to be safe against quantum attacks

Can start post-quantum planning and testing *now*



Open Quantum Safe Project

Use in applications

Apache httpd

nginx

curl, links

Open VPN

Chromium

Integration into forks of widely used open-source projects

OpenSSL
- TLS 1.2
- TLS 1.3

BoringSSL

Open SSH

Language SDKs
C#, C++, Go, Python

C language library, common API
- x86/x64 (Linux, Mac, Windows)
- ARM (Android, Linux)

liboqs

key exchange / KEMs

signatures

isogenies

code-based

lattice-based

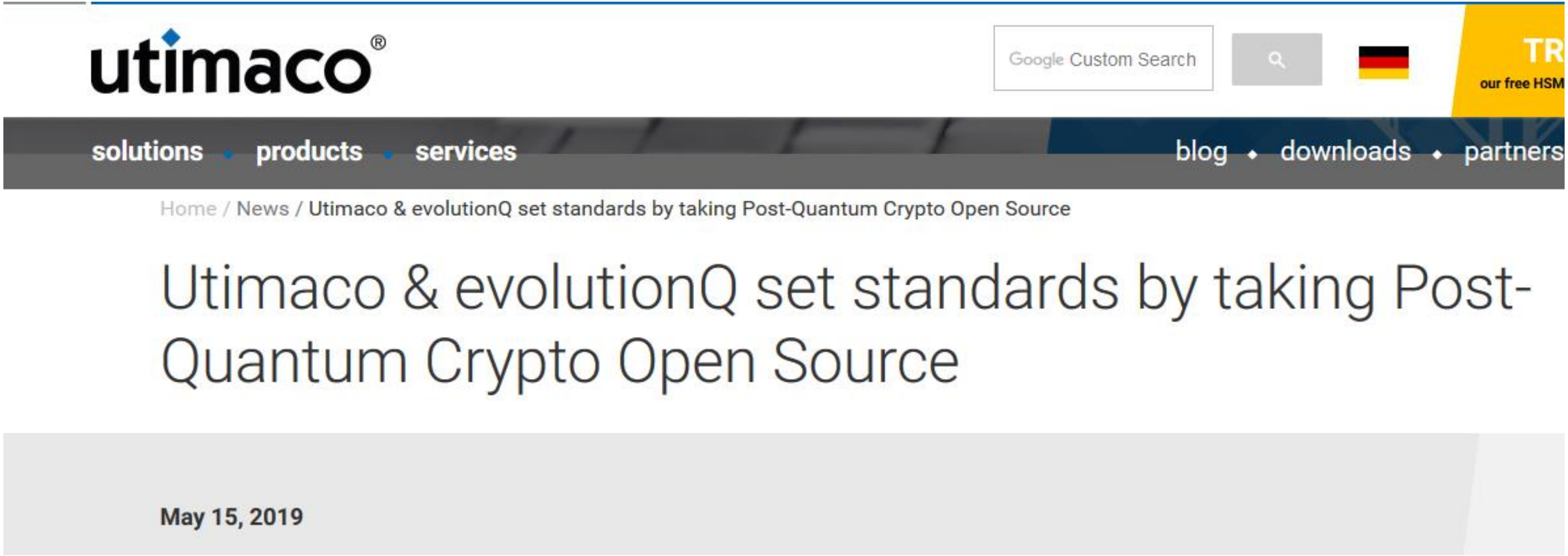
multi-variate polynomial

hash-based / symmetric

Standalone C reference implementations, heavily tested

PQClean

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

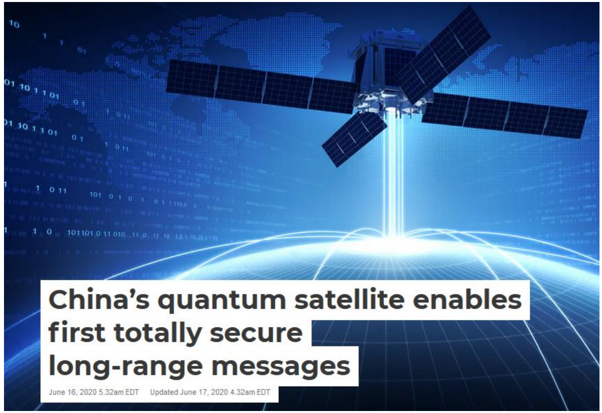


Home / News / Utimaco & evolutionQ set standards by taking Post-Quantum Crypto Open Source

Utimaco & evolutionQ set standards by taking Post-Quantum Crypto Open Source

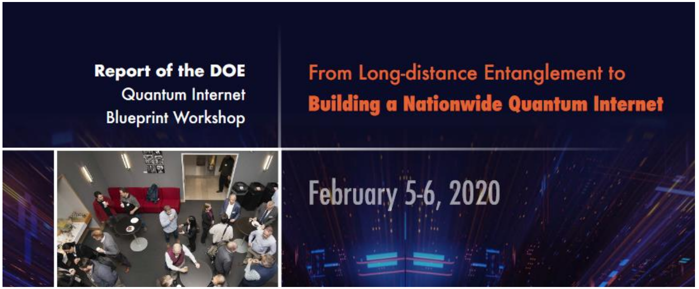
May 15, 2019

Toward large scale quantum communication networks



China's quantum satellite enables first totally secure long-range messages

June 16, 2020 5.32am EDT Updated June 17, 2020 4.32am EDT



Report of the DOE
Quantum Internet
Blueprint Workshop

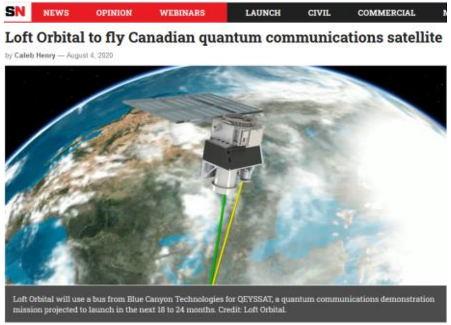
From Long-distance Entanglement to
Building a Nationwide Quantum Internet

February 5-6, 2020

https://www.energy.gov/articles/quantum-internet-future-here

EvolutionQ Awarded Contribution From Canada Space Agency for Quantum Key Distribution Network Research and Development

August 15, 2020



Loft Orbital to fly Canadian quantum communications satellite

by Caleb Henry — August 4, 2020

Loft Orbital will use a bus from Blue Canyon Technologies for QEYSSAT, a quantum communications demonstration mission projected to launch in the next 18 to 24 months. Credit: Loft Orbital.

Chinese scientists report breakthrough on quantum internet technology with entangled atoms

- Paper in the journal 'Nature' says team was able to 'entangle' two clouds of atoms via a 50km optical fibre
- It was the longest distance photons have travelled in such an experiment

Stephen Chen in Beijing
Published: 11:00pm, 14 Feb, 2020

South China Morning Post

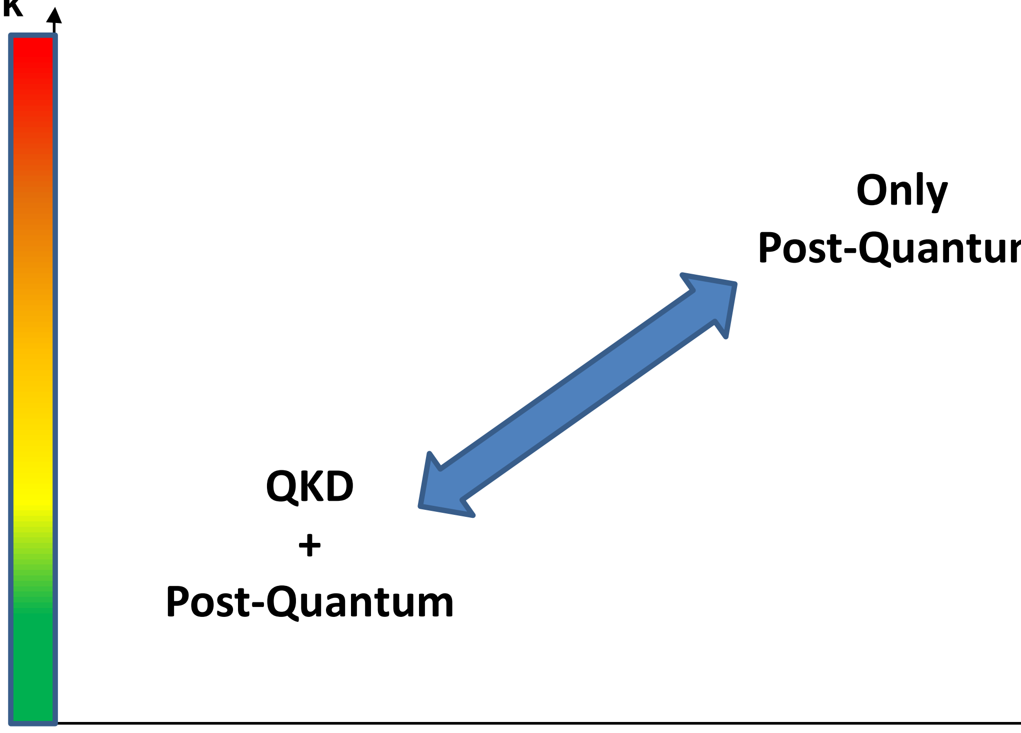
European Commission > Strategy > Shaping Europe's digital future > News >

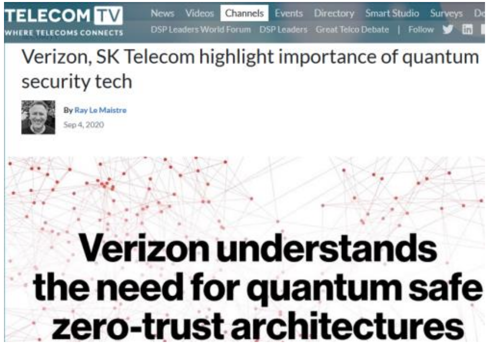
Shaping Europe's digital future

DIGIBYTE | 13 June 2019

The future is quantum: EU countries plan ultra-secure communication network

Risk vs convenience



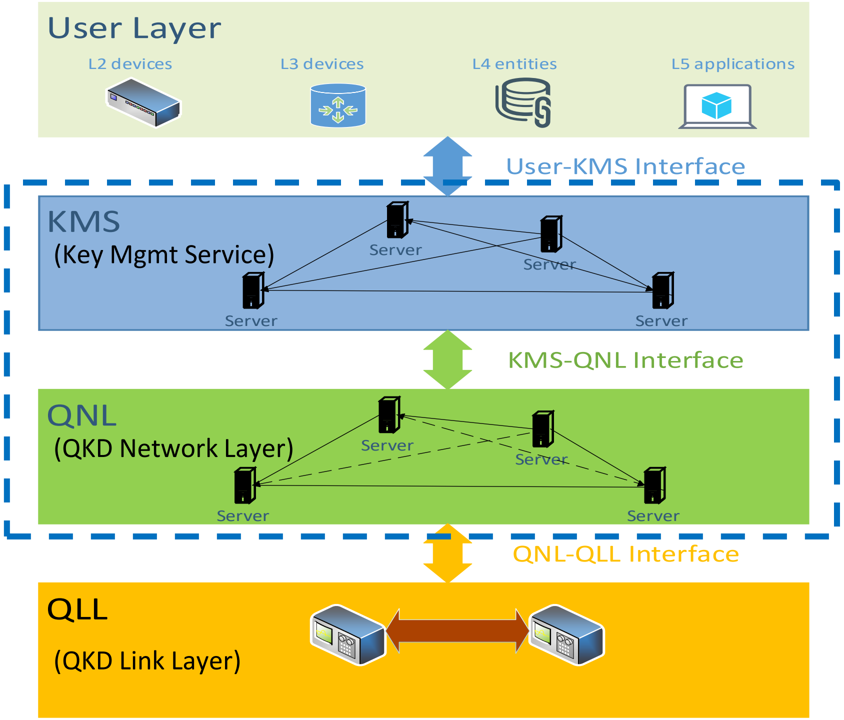


Verizon, SK Telecom highlight importance of quantum security tech

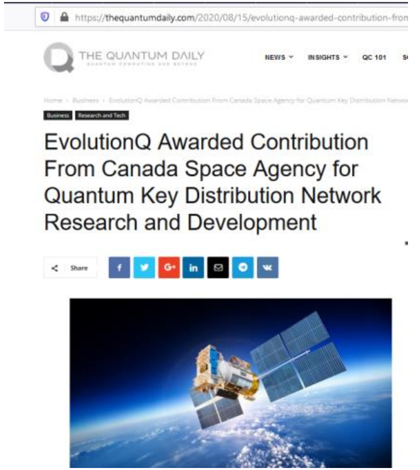
By Ray Le Maistre
Sep 4, 2020

Verizon understands the need for quantum safe zero-trust architectures

Designing quantum key agreement into systems *now*



- Layered architecture
  - Introduce QKD Networking into an <u>existing</u> Network & Key Management Environment
- Standards compliance
  - Contributing to ETSI and ITU-T standards
- Technology Readiness
  - Evaluate Opensource QKD Networking Today : OpenQKDNetwork.ca
  - evolutionQ QKD Network Commercial Product available 2020.
- QKD tech agnostic
  - Expand a QKD Network over time with different vendors.



https://thequantumdaily.com/2020/08/15/evolutionq-awarded-contribution-fron

THE QUANTUM DAILY

QUANTUM COMPUTING AND BEYOND

NEWS INSIGHTS QC 101

Home › Business › EvolutionQ Awarded Contribution From Canada Space Agency for Quantum Key Distribution Networ

Business Research and Tech

EvolutionQ Awarded Contribution From Canada Space Agency for Quantum Key Distribution Network Research and Development

Share

KEEP

CALM

& build

BACK

better

Build greater resilience against cryptanalytic attacks

Yesterday

Today

Soon
(hybrid, agile,
post-quantum)

Soon after
(hybrid, agile,
post-quantum
+QKD)

2021 Resolutions

- Put someone in charge of producing a quantum readiness plan by Q2
- Provide them broad executive support for the planning exercise
- Engage relevant standards organizations by Q3
- Update RFPs and start engagement by Q4

evolution

Prepare for the Quantum Age.

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

Quantum-Safe Strategy Workshops & Advisory

Quantum Risk Assessments

Quantum-Safe Research & Verification

QKD network software

Post-quantum software long-term support