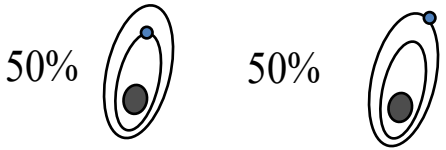
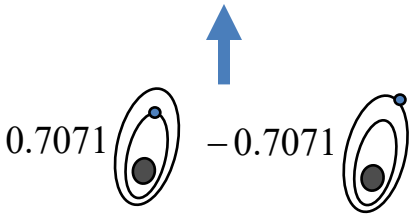
Resilienza e prosperità nell'era quantistica

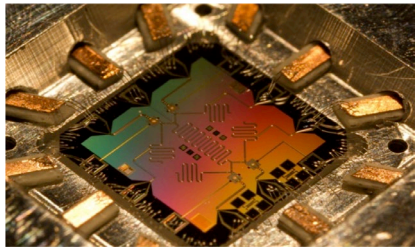
Michele Mosca

6 ottobre 2022

evolution

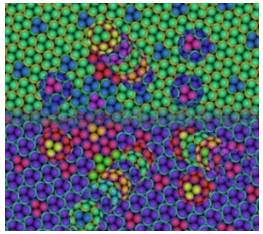




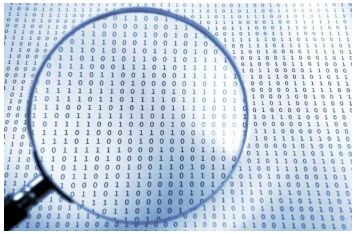


# qubits	#classical numbers to store
3	$8=2^3$
4	$16=2^4$
10	$1024=2^{10}$~Kilo
20	$1048576=2^{20}$~Mega
30	$1073741824=2^{30}$~Giga
40	$1099511627776=2^{40}$~Tera
50	$1125899906842624=2^{50}$~Peta
60	$1152921504606846976=2^{60}$~Exa
70	$1180591620717411303424=2^{70}$~Zetta
128	$340282366920938463463374607431768211456=2^{128}$~$3.4\times10^{38}$
230	$1725436586697640946858688965569256363113277724304259663879063105594 9824=2^{230}$~$10^{100}$

New paradigm brings new possibilities



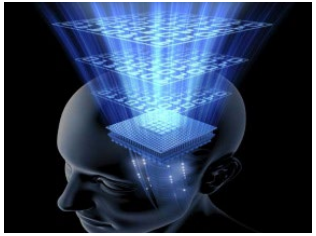
Designing new materials, drugs, etc.



Optimizing

Sensing and measuring

Secure communication



What else???

What sorts of practical applications?

Possibilities include:

- Optimizing the design of new materials

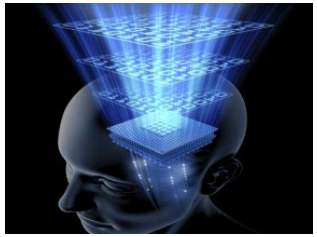
For example, next generation materials could allow more efficient energy capture or transport or storage.

- Simulating chemical reactions at the quantum level

Potential applications include more efficient yields for chemical processes like the production of fertilizers.

- Optimization of designs or allocation or resources

For example, optimizing in the insertion of dampers in buildings to protect against earthquakes.



What else???

Exploring a range of optimization problems in industry

Impact on any specific problem/sector?

Possibilities include:

- None at all.
- *10% improvement*
- *1000% improvement*
- *Transformational*

Can unexpectedly and rapidly jump from one category to another.

Detailed and ongoing assessment is needed for each sector.

Are you a provider of technology impacted by quantum? And/or a user?

For users: do you want to depend on vendors who are not ready?

IBM

IBM Newsroom | Home | Latest News | Press Releases | Media Contacts | Media Center | Leadership | Global Newsrooms

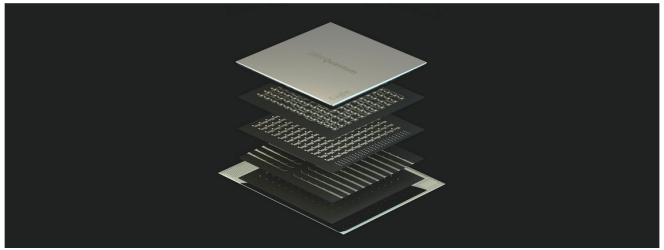
IBM Unveils Breakthrough 127-Qubit Quantum Processor

- Delivers 127 qubits on a single IBM quantum processor for the first time with breakthrough packaging technology

- New processor furthers IBM's industry-leading roadmaps for advancing the performance of its quantum systems

- Previews design for IBM Quantum System Two, a next generation quantum system to house future quantum processors

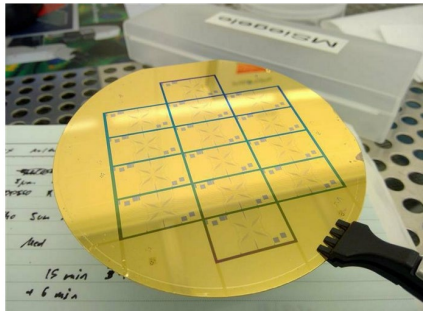
Nov 16, 2021



Universal Quantum

Feb 22 · 5 min read

How Universal Quantum is rising to the million-qubit challenge



Honeywell

Industries

Honeywell Quantum Solutions

Honeywell Quantum Solutions and Cambridge Quantum have combined to form Quantinuum – the world's largest integrated quantum computing company.

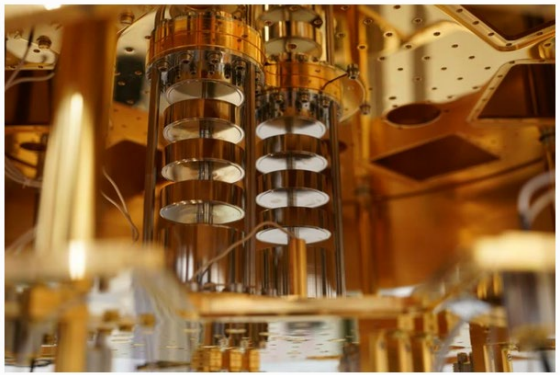
THE WALL STREET JOURNAL.

SUBSCRIBE | SIGN IN

Forbes

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

Intel Advances On The Road To Quantum Practicality



rigetti

Rigetti Computing Announces Commercia

Rigetti Computing Announces Commercial Availability of 80-Qubit Aspen-M System and Results of CLOPS Speed Tests

February 15, 2022 09:00 ET | Source: Supernova Partners Acquisition Company II

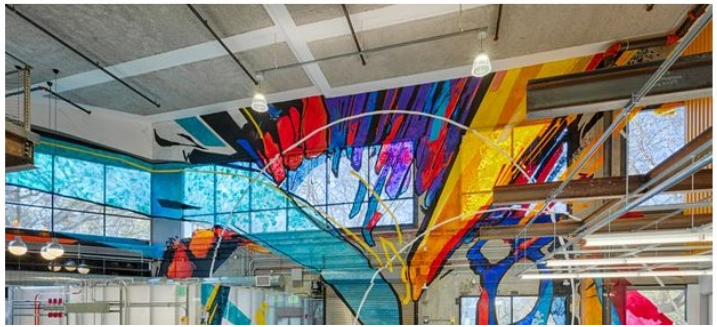
COLLEGE PARK, MD — FEBRUARY 23, 2022

IonQ Aria Furthers Lead As World's Most Powerful Quantum Computer.

CIO JOURNAL

Google Aims for Commercial-Grade Quantum Computer by 2029

Tech giant is one of many companies racing to build a business around the nascent technology



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

'he country wants to build a quantum computer with a million times the computing power resently in the world.

y 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

SHARE

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

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.

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.

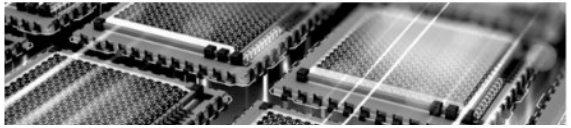
Microsoft Azure

Azure Quantum

Build quantum solutions today

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

January 9, 2019 Nicole Hemsoth



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

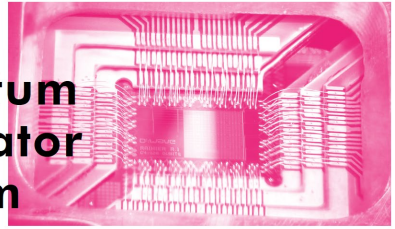
www.quantumindustrycanada.ca

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

CREATIVE DESTRUCTION Lab

About the Program Streams Companies Locations Blog Apply

CDL Quantum Incubator Stream



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

THE QUANTUM DAILY

QUANTUM COMPUTING AND BEYOND

NEWS INSIGHTS

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

July 2, 2020

AIRBUS

Commercial Aircraft Helicopters

Airbus Quantum Computing Challenge

Bringing flight physics into the Quantum Era

siliconANGLE

UPDATED 10:45 EDT / SEPTEMBER 29 2020

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

BY MIKE WHEATLEY

softwareQ

DESIGNING QUANTUM SOFTWARE

staq - A full-stack quantum processing toolkit

Matthew Amy[*1,3] 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

[4]Department of Combinatorics and Optimization, University of Waterloo, Waterloo ON, Canada

Version of December 11, 2019

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

PLoS ONE 13(12): e0208073 (2018)

Cyber attacks

www.theglobeandmail.com/business/commentary/article-the-quantum-threat-to-cybersecurity-danger-meets-opportunity/

THE GLOBE AND MAIL

OPINION

The quantum threat to cybersecurity: Danger meets opportunity

TIFF MACKLEM, MICHELE MOSCA, BRIAN O'HIGGINS
CONTRIBUTED TO THE GLOBE AND MAIL
PUBLISHED MAY 6, 2019

Cloud computing, Sistemi di Pagamento,
Internet, IoT, etc…

Navigazione sicura, Update automatici, VPN,
Email sicura, Blockchain, etc…

Crittografia: RSA, DSA, ECDSA,…, SHA, AES

Ma ci sono così tante vulnerabilità!

- Fundamentally vulnerable cryptography
- Cryptography implementation errors
- User errors
- Platform implementation errors
- Platform design errors
- Admin errors
- Corrupt users
- Corrupt admin

Classificati, da male a peggio?

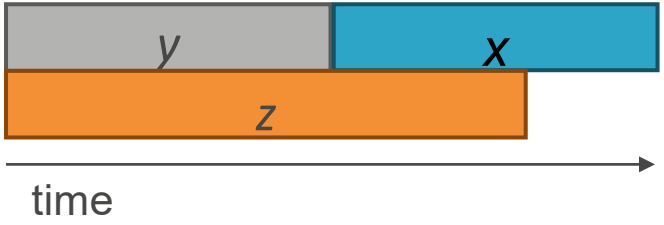
- User errors
- Corrupt users
- Admin errors
- Corrupt admin
- Platform implementation errors
- Platform design errors
- Crypto implementation errors
- **Fundamentally vulnerable cryptography**

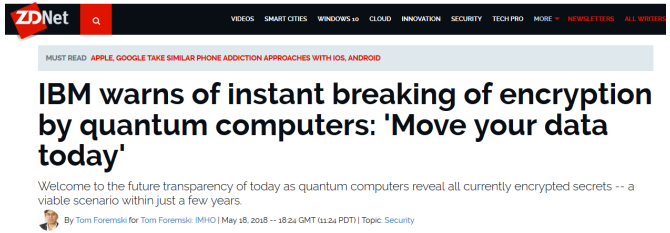
Ma dobbiamo preoccuparci *adesso*?

Depends on*:

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

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




ZDNet

VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS ALL WRITERS

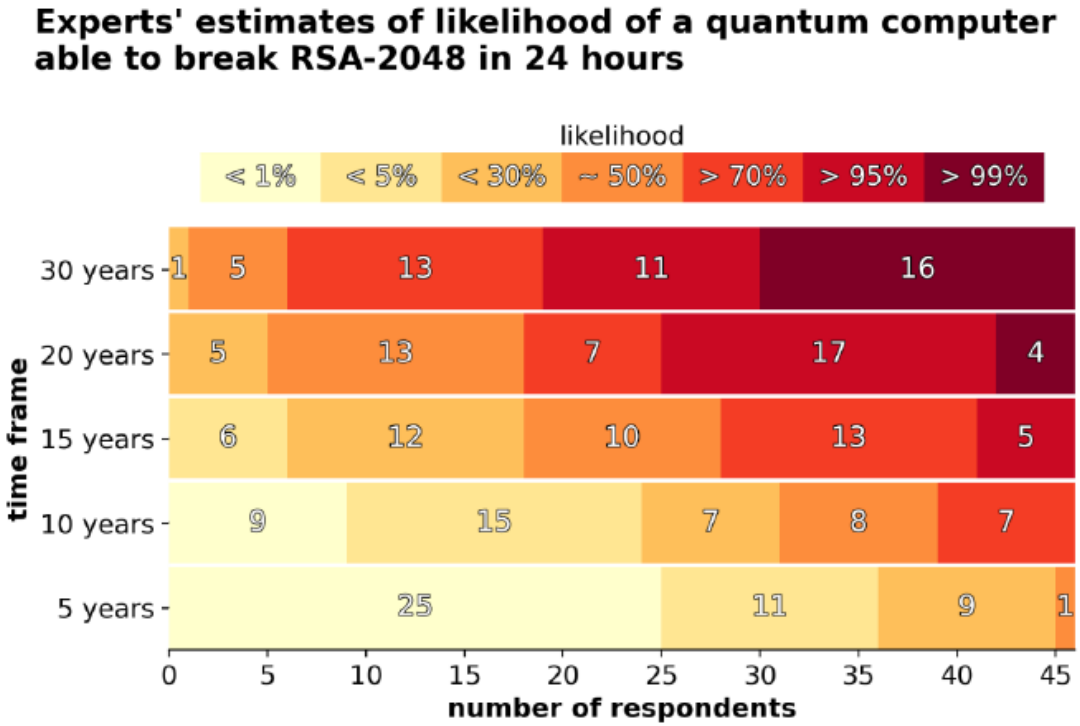
MUST READ APPLE, GOOGLE TAKE SIMILAR PHONE ADDICTION APPROACHES WITH IOS, ANDROID

IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'

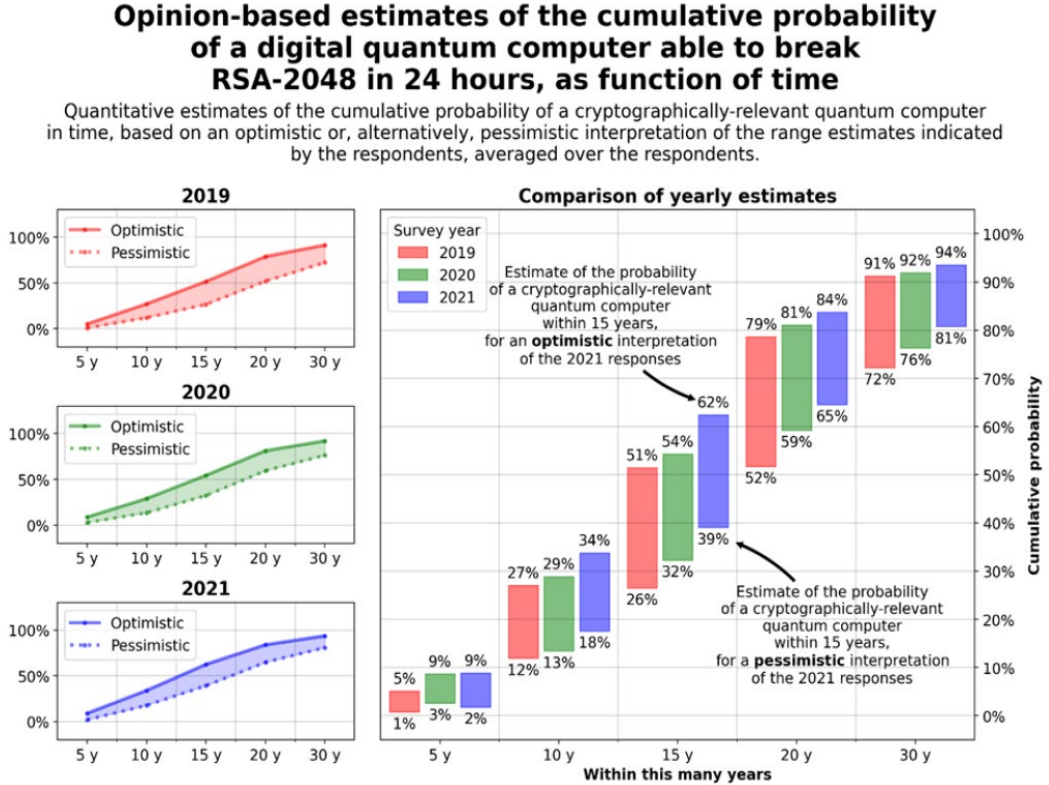
Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years.

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



https://globalriskinstitute.org/download/quantum-threat-timeline-report-2021-full-report/



https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

INTERNATIONAL
CRYPTOGRAPHIC
MODULE CONFERENCE 2022
September 14-16 | Westin Arlington Gateway, Virginia, USA

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

Strumenti per crittografia *quantum-safe*

Crittografia tradizionale quantum-safe

nota come **crittografia post-quantum**
o Algoritmi Quantum-Resistant

Crittografia quantistica

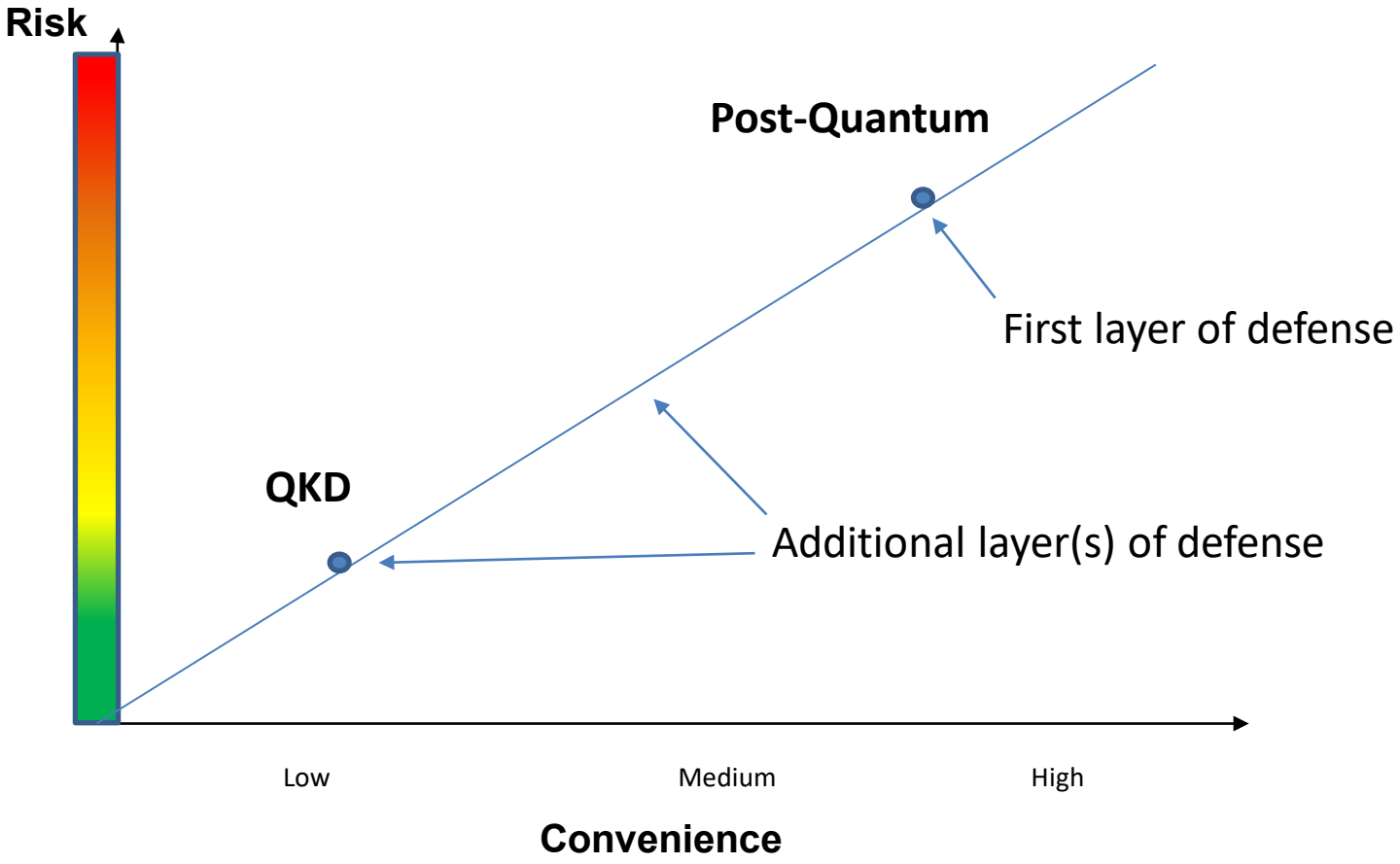
nota anche come **distribuzione di chiavi quantistica**
(Quantum Key Distribution - QKD)

Courtesy of Qiang Zhang, USTC

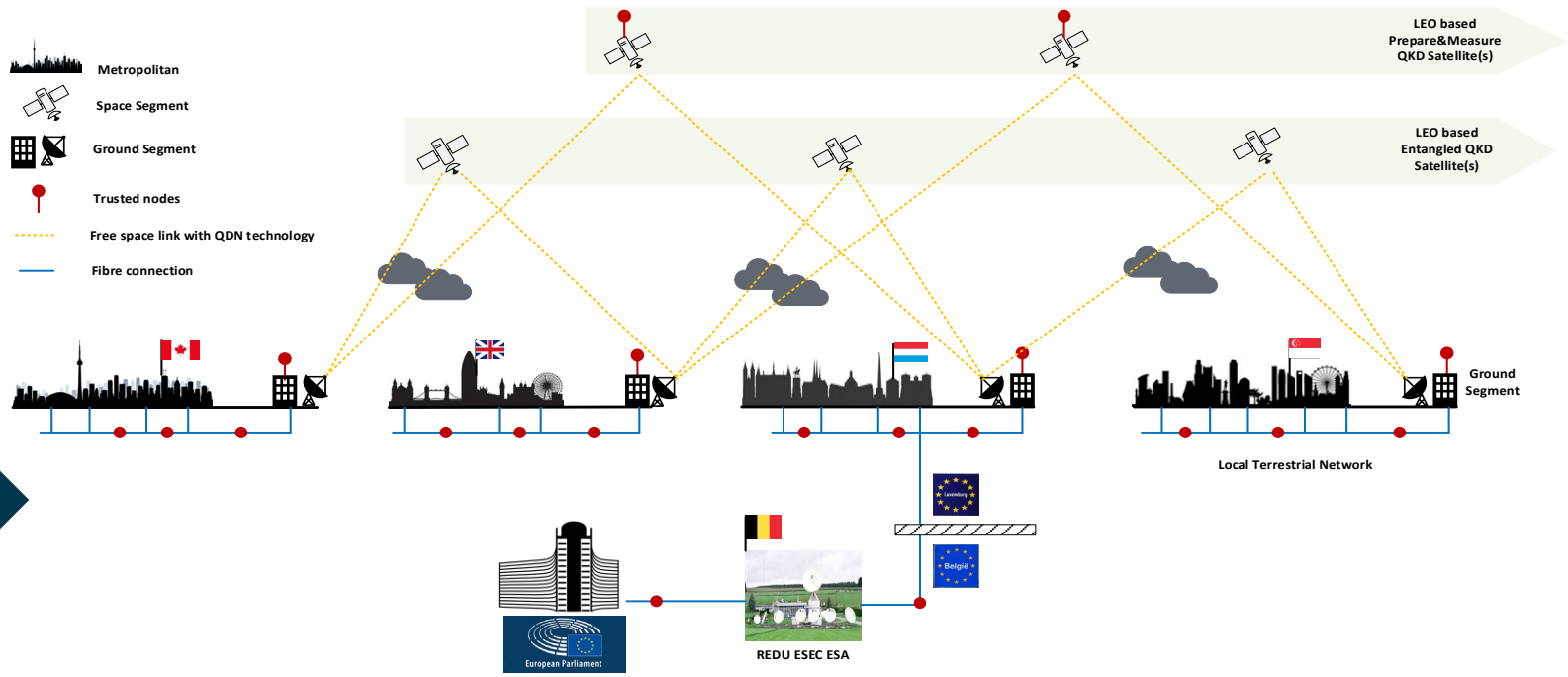
http://www.idquantique.com/photon-counting/clavis3-qkd-platform/

Questi strumenti posso essere adottati entrambi
e lavorare bene assieme in un singolo sistema quantum-safe

Risk vs convenience



INT-UQKD DEMOs (Roberto Mazzolin)



Demonstration 1: Demonstrating a Pilot Use case over a fibre-based Terrestrial network between Belgium (ESEC ESA REDU) and Luxembourg

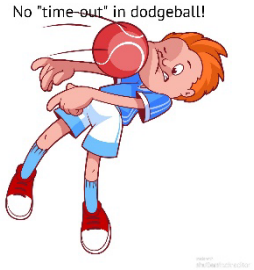
Demonstration 2: Demonstrating a Luxembourg-Canada-Singapore Pilot Use case employing a hybrid Space-Terrestrial network established through fibre-based and satellite communication infrastructures

Demonstration 3: Demonstrating a Pilot Use case over Belgium (ESEC ESA REDU) and United Kingdom (ESA ECSAT Harwell) considering a hybrid Space-Terrestrial network

Demonstration 4: Demonstrating Pilot use case considering Canada - United Kingdom (ESA ECSAT Harwell) using a hybrid fibre-based and satellite communication infrastructure.

Demonstration 5: Assess the inter-connection of INT-UQKD Pilot Use case with other national and international QCI initiatives

“Execution is 90% planning and 10% doing”



We don’t get to call a “time-out” if we’re not ready!

1. Perdita di riservatezza e di integrità dei dati
2. Infrastrutture critiche interrotte, senza possibilità di ripristino immediato
3. Tentativi affrettati di preparazione:
   - sono costosi
   - rischiano di fare danni
   - possono aprire nuove falle di sicurezza
4. Perdita di fiducia negli strumenti e nelle istituzioni alla base della nostra economia digitale

Approaching “show-time”!

NIST IR 8413 Third Round Status Report

Table 4. Algorithms to be Standardized

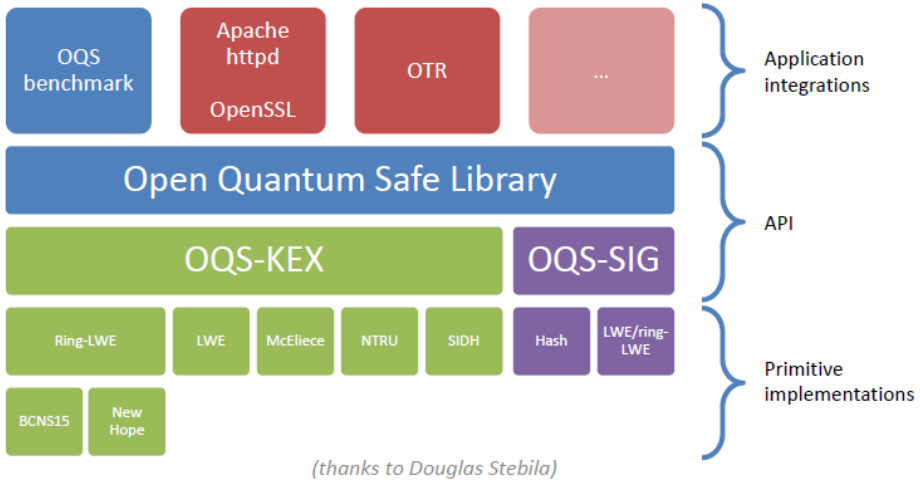
Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Table 5. Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	Digital Signatures
BIKE	
Classic McEliece	
HQC	
SIKE	

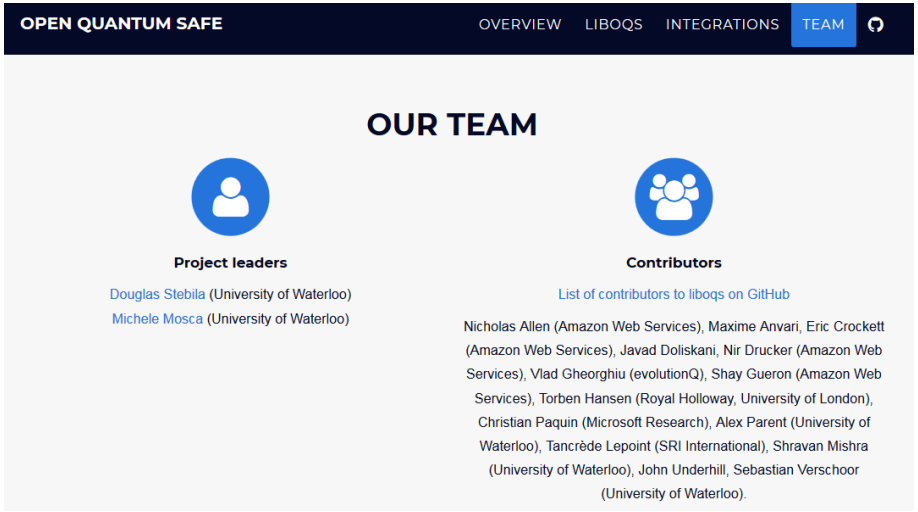
https://doi.org/10.6028/NIST.IR.8413

E’ possible testare *ora* l’implementazione di algoritmi post-quantum



(thanks to Douglas Stebila)

openquantumsafe.org



Altre implementazioni open-source:
https://github.com/mupq/pqm4
https://libpqcrypto.org
https://github.com/safecrypto/libsafecrypto
Sono disponibili anche tool-kit commerciali

Encouragement and best-practices: DHS on Preparing for PQC

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Issue Date: 09/17/2021
Expiration Date: (two years after issued date)

Policy Directive 140-15

MEMORANDUM FOR: Distribution

FROM: Eric Hysen
Chief Information Officer

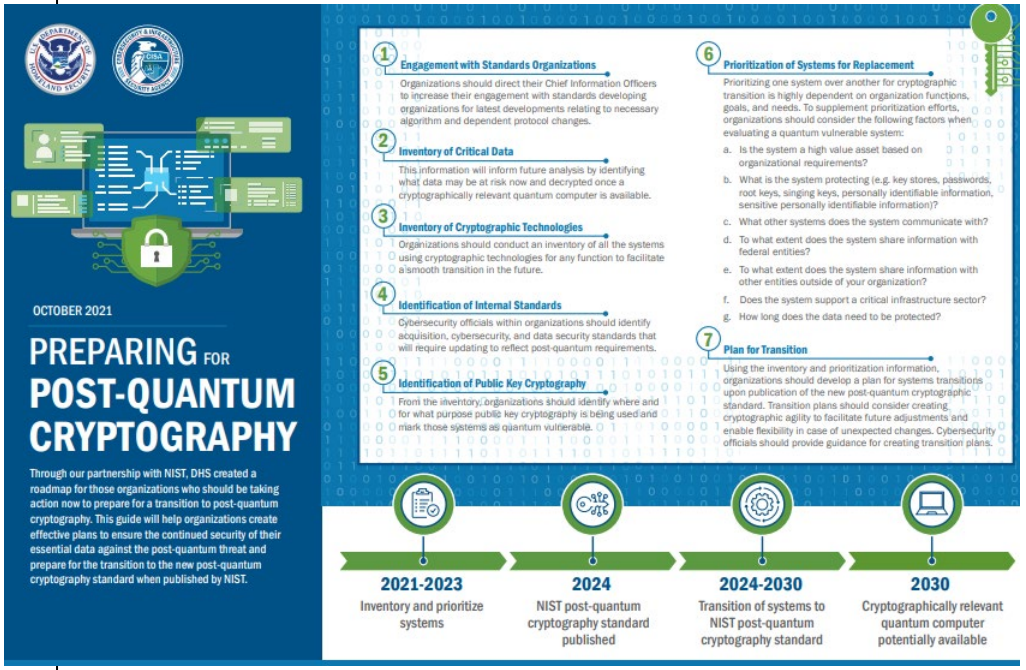
SUBJECT: Preparing for Post-Quantum Cryptography

Purpose: DHS has significant national security concerns across mission spaces including critical infrastructure, law enforcement, privacy, and counterintelligence that could be harmed by insufficient preparation for a transition to post-quantum cryptography. This memorandum provides guidance to Component Heads to begin preparing for a transition from current cryptography standards to post-quantum encryption now to mitigate risks to data and mission functions.

This memorandum provides Component Heads with an overview of some specific risks to the DHS mission, and a roadmap to take action against the quantum threat to current cryptographic systems. While there is no U.S. Government-approved post-quantum cryptographic standard as of the release of this Statement, these preparatory steps will significantly reduce the time required for transition once industry adopted and U.S. Government validated algorithms are available, resulting in continued mission success and a more secure homeland.

The threat posed to current cryptographic methods extends beyond the Department, affecting interagency, international, and private sectors partnerships critical to mission success. The roadmap below should be used by Components to encourage effective and consistent transition preparation among DHS partners. The potential costs of a slow or ineffective transition to post-quantum cryptography present significant threats to DHS operations and the security of the

https://www.dhs.gov/quantum



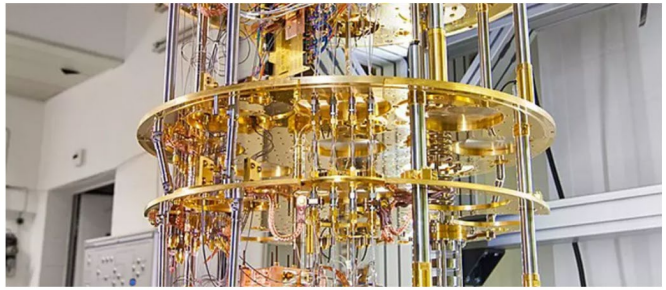
Agenda Events Reports Platforms

WORLD ECONOMIC FORUM

MY FORUM Join u

Quantum Computing | Cybersecurity

How the world can prepare for quantum-computing cyber risks



Quantum computing is soon to become a technology of the present. Image: IBM Zurich Lab/Creative Commons

28 Sep 2021

Colin Soutar
Managing Director, Cyber Risk, Deloitte

Isaac Kohn
Partner, Deloitte

Itan Barmes
Manager, Deloitte and Project Fellow, Quantum Security, World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum

Sean Doyle

AUDIO: LISTEN TO THE ARTICLE

-08:42

This is an experimental feature. Some words or names may be mispronounced. Does it sound good? Yes / No

- Futuristic quantum computing will soon become the technology of the present.
- It will be a positive advancement for many disciplines, but the potential security impacts are generally not fully understood by citizens, organizations, or decision-makers.
- These different audiences need tailored messaging to enable a collective and coordinated

LLOYD'S

There are many insurance lines of business that will be impacted by the emergence of quantum computing. However, the largest potential impact arises from the **cyber** security risks posed by cryptographically relevant quantum computers. Cyber risks by their nature can have an influence on many lines of insurance business and practically all industries. In a scenario where the cryptographic threat from quantum computing precedes the full adoption of PQC or other quantum-secure protocols, the world and the insurance industry face a systemic cyber risk that can affect everything from the security of our text messages to state guarded secrets and access to military codes.

Quantum computing also exacerbates the risk faced by AI technology, since quantum computing will improve ML capabilities, leading to a broader adoption of ML and AI solutions and products in all industries. The impacts of AI on insurance are further discussed in the Lloyd's report *Taking control: AI and insurance*.[1] The following are few examples of insurance lines of business that can be impacted by quantum computing:

- **Product liability and product recall**: Liability arises from AI-based machinery and products making a mistake. Whilst the risk of AI malfunction increases once more AI reliant products enter the market as a result of improved ML capabilities, quantum computing will also most likely improve the accuracy of AI as larger data sets can be processed to train ML algorithms. Therefore, the product liability and product recall risk landscape of robots and AI products will be changed with the emergence of quantum computing.
- **Third-party motor liability**: The liability complications arising from accidents involving autonomous vehicles will become a reality sooner than expected, with ML based quantum computing accelerating the arrival of driverless cars.
- **Political risks**: The power of quantum computing could lead to the creation of better deep fakes, be used to better distribute online propaganda and fake news and take advantage of human behaviour for social engineering. This increased capability to instigate political unrest can lead to more protests, followed by government backlash, which would have an impact on business interruption and property damage.
- **Property damage**: The expensive hardware and control systems employed in quantum computing mainframes will increase the property risk profile.

Insurance lines of business affected

Systemic cyber risk

Sate sponsored cyber attacks using a quantum computer could be used to break RSA and forge digital signatures. This would allow adversaries access to private and public networks where they could spread malware to dismantle critical infrastructure. Falsified information could be spread using the accounts of high profile figures. Unsolicited access to weaponry and nuclear codes could be used to wreak havoc. Classified data held by the military could be decrypted and all operations, whether on land, in sea or in space would be vulnerable as global networks would be compromised (systemic **political risk** impact).

Other nefarious adversaries, including fraudulent employees (**fidelity risk**), could access or alter personal, legal, operational or financial data. The PKI, used to distribute private keys and digital authentication certificates in military agencies and many large organisations including financial institutions, would come under attack. This would allow the forgery of common assess cards (CAC) which are required to access classified networks and data.[2] Trade secrets and **IP** could be stolen (some nation states already use IP attacks as part of their economic strategy). The security behind robots and IoT devices, which are likely to be employed on a wider scale due to AI improvements offered by quantum computing, would be compromised. This would allow large scale supply chain disruptions (**(contingent) business interruption**). Autonomous vehicles could be hacked to divert their path and cause accidents (**third-party motor liability**). 3D printers and manufacturing machinery connected to the internet could be tampered with, leading to large scale **product liability** and **product recall** claims. The blockchain technology underpinning **cryptocurrencies** could be manipulated to alter or forge transactions and double spend money. The privacy of civilian messages, photos and medical data would also be compromised. Insurance institutions might be particularly targeted as they hold vast amounts of sensitive policyholder data, resulting in hefty **GDPR fines**.

As a result, quantum computing could pose one of the largest scale systemic risks in history. With the ever increasing interconnectedness of systems and our reliance on digital communications, a technology capable of breaking the very encryption system behind our cyber security protocols would have implications that affect every aspect of our lives, from state security, to the privacy of our text messages.

Information at risk from cryptographically relevant quantum computing

Source: (1) Lloyd's, 2019 (2) Lindsay, 2020

https://lloydslab.com/wp-content/uploads/Quantum-Paper.pdf

Canadian National Quantum-Readiness Best Practices and Guidelines

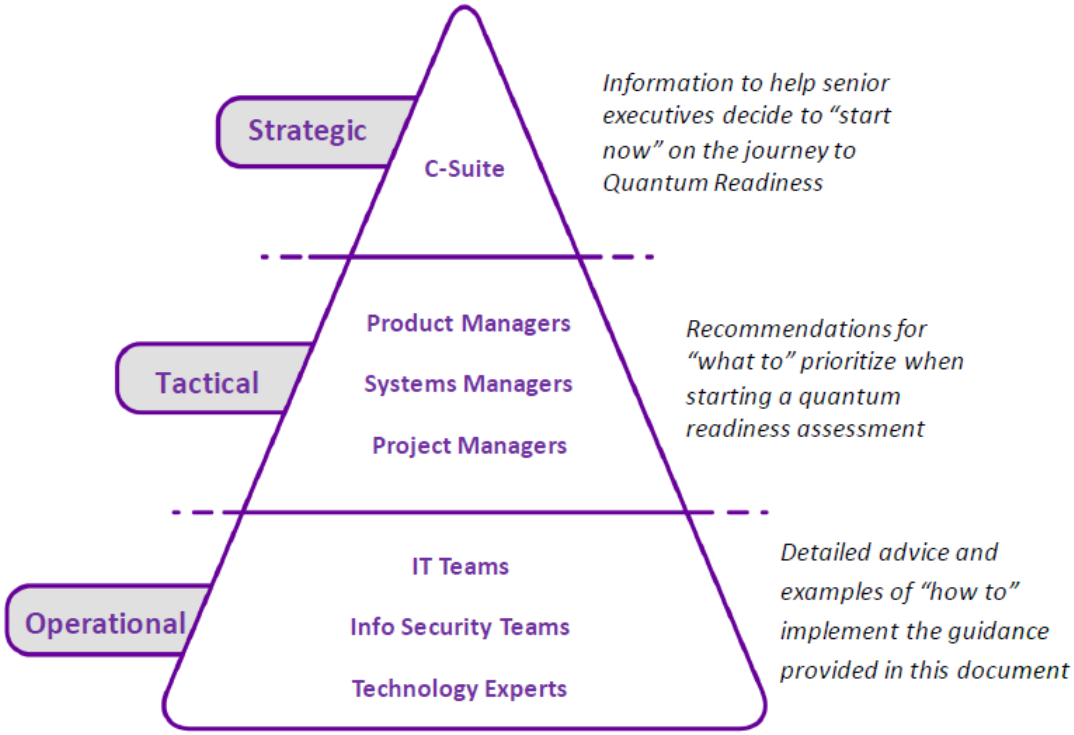
Government of Canada / Gouvernement du Canada

Canadian Forum for Digital Infrastructure Resilience (CFDIR)

https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11618.html

CFDIR working groups implement agreed-upon projects. Current focus areas include:

- Cloud Security
- Quantum Readiness
- IoT Security
- Supply Chain Assurance
- Internet Resilience
- Rapid Response (e.g. to the COVID-19 pandemic)


Strategic
C-Suite
Information to help senior executives decide to "start now" on the journey to Quantum Readiness
Tactical
Product Managers
Systems Managers
Project Managers
Recommendations for "what to" prioritize when starting a quantum readiness assessment
Operational
IT Teams
Info Security Teams
Technology Experts
Detailed advice and examples of "how to" implement the guidance provided in this document

FOREWORD

The Bank of Canada is committed to working with its public- and private-sector partners to promote and strengthen the resilience of Canada's financial sector in the face of risks to business operations, including cyber incidents.

That's why we were pleased to take part in the Quantum-Readiness Working Group (QRWG) launched in 2020 by the Canadian Forum for Digital Infrastructure Resilience (CFDIR). A team of subject matter experts from organizations responsible for core elements of Canada's financial critical infrastructure has been studying what it will take to make Canada "quantum ready" in the years ahead.

The key message I want to leave you with is that we all need to start preparing now. The encryption technologies that are securing Canada's financial systems today will one day become obsolete. If we do nothing, the financial data that underpins Canada's economy will inevitably become more vulnerable to cyber criminals.

While some still see quantum as a long way off—given that this advanced encryption technology is not yet available—we also know that it will take time to develop and implement the quantum-safe encryption systems to replace those we have now.

The information and recommendations you see in this document were assembled and developed by people who are responsible for making these kinds of changes in their own institutions. The concepts are fundamental—with application to both small and large organizations, in both the public and private sector settings.

It starts with assessing the potential impact of quantum on your own organization. In addition to risks, quantum may also present opportunities. But no matter what, we all need to prepare for this transition—including in my own organization, the Bank of Canada. The resilience of Canada's financial system depends on it.

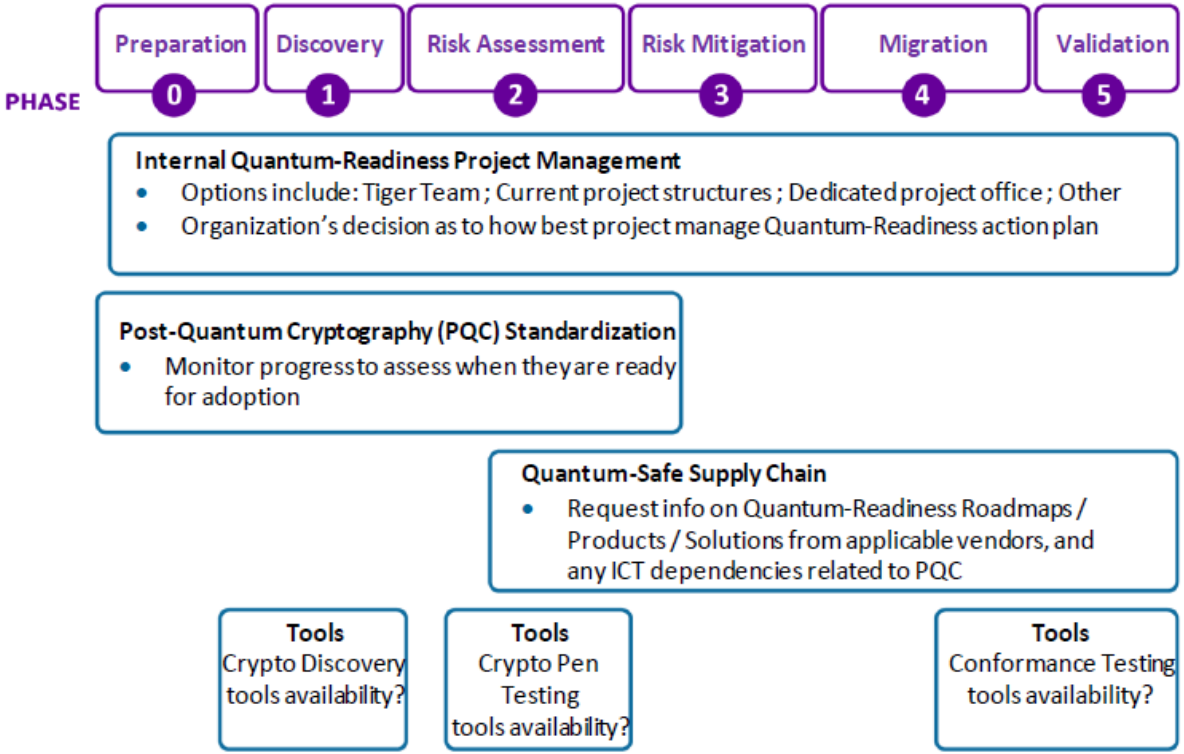
We would like to thank our colleagues who took part in this initial pilot project. There is a long road ahead, and the Bank of Canada will be there alongside our partners as the quantum issue unfolds.

Hisham El-Bihbety

CISO – Bank of Canada

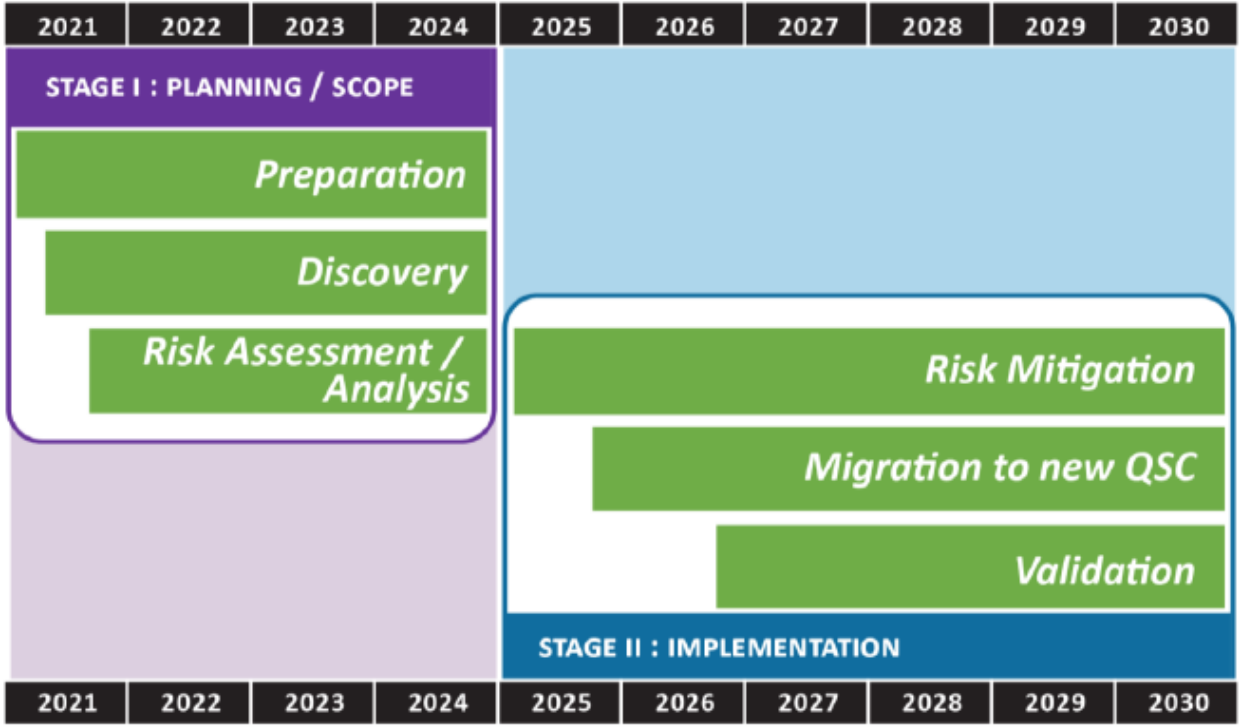
Quantum-Readiness Program Elements

Some Conceptual Building Blocks



Quantum-Readiness Program Timeline

Initial Recommendations as of June 2021



Metodologia per la valutazione del rischio quantistico

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

Fase 1 Identificare e documentare le risorse da proteggere e il loro presente grado di protezione crittografica

Fase 2 Valutare lo stato di sviluppo delle tecnologie quantistiche, e l'orizzonte temporale per lo sviluppo dei computer quantistici

Fase 3 Identificare e documentare le possibili minacce e l'orizzonte temporale ***Z*** in cui i malintenzionati potrebbero avere accesso alla necessaria tecnologia quantistica

Fase 4 Identificare il tempo di conservazione ***X*** desiderato per le risorse/dati da proteggere, e il tempo di migrazione ***Y*** necessario per implementare la transizione dell'infrastruttura dell'organizzazione a una condizione di non-vulnerabilità (*quantum-safe state*)

Fase 5 Determinare il rischio quantistico calcolando se le risorse da proteggere potrebbero diventare vulnerabili ad un attacco quantistico prima che la transizione sia implementata:

$$X + Y > Z \ ?$$

Fase 6 Identificare e dare priorità alle attività necessarie per mantenersi informati su sviluppi tecnologici rilevanti, e per rendere la tecnologia dell'organizzazione quantum-safe

Build greater resilience against cryptanalytic attacks

Yesterday

Today

Tomorrow

Thank you! Grazie!

Domande e commenti sono benvenuti!

@evolutionQinc

Michele Mosca

CEO, evolutionQ Inc.

michele.mosca@evolutionq.com

Geschäftsführer, evolutionQ GmbH

michele.mosca@evolutionq.de

https://evolutionq.com/