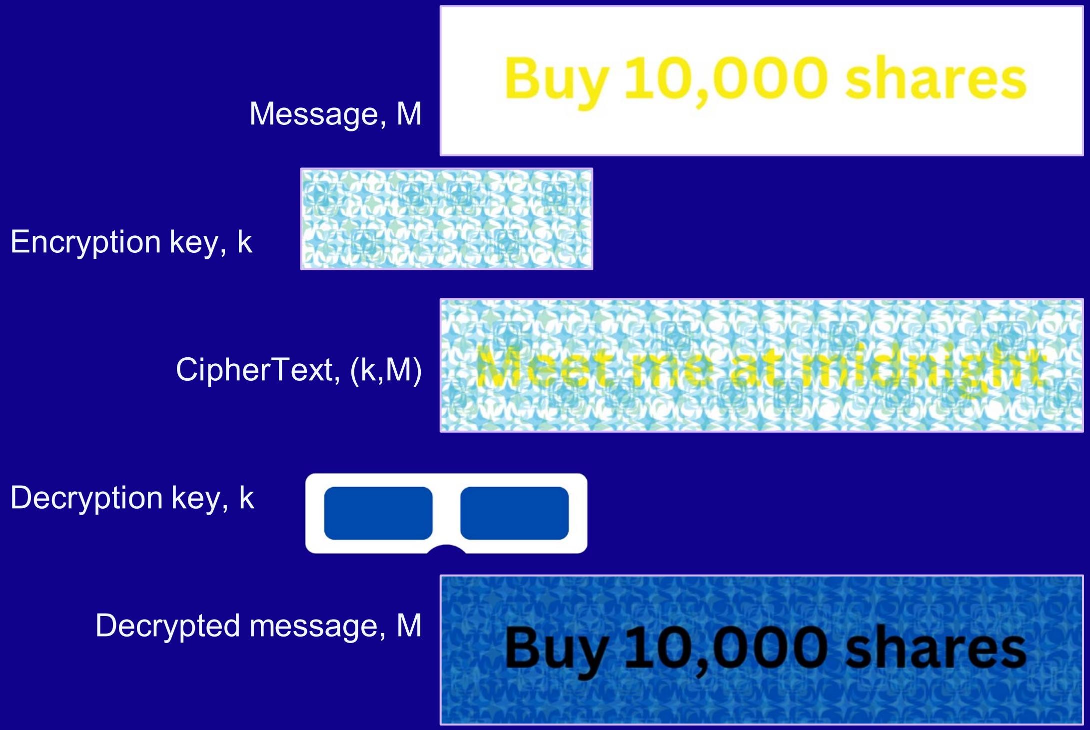
Quantum Computing for Business Executives

13 February 2023 - 9th ETSI-IQC Quantum-Safe Cryptography Workshop - Michele Mosca

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing
PERIMETER INSTITUTE FOR THEORETICAL PHYSICS
evolution

How can we entrust information and tasks to untrusted systems?

Quantum Changes what is “Secure”



Quantum Changes Everything




Key Establishment

Symmetric Encryption

Authentication

New Paradigm

Each classical configuration has a corresponding quantum amplitude

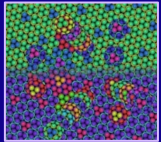
Number of bits	Possible configurations	What are the possible configurations?
1	2	
2	$2^2 = 4$	
8 = 1 byte	$2^8 = 256$	etc
10	$2^{10} = 1024$	Far too many to show
1,000,000 = 1 megabit	$2^{1,000,000}$	

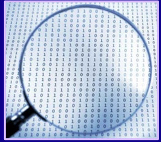
New Paradigm

Number of **qu**bits	Amplitudes to track	Classical bits to keep track of with non-zero amplitudes
1	2	2
2	2^2	2^2
3	2^3	$2^3 = 8 \rightarrow 1$ byte
10	2^{10}	$2^{10} = 1{,}024 \rightarrow \sim 1$ kilobit
20	2^{20}	$2^{20} = 1{,}048{,}576 \rightarrow \sim 1$ megabit
40	2^{40}	$2^{40} = 1{,}099{,}511{,}627{,}776 \rightarrow \sim 1$ terabit

If we use k bits of precision to store a single amplitude, we need approximately $k\,2^N$ bits to describe the state of N qubits: **exponential** growth (in the number of qubits)

Quantum brings immense power


Material and pharmaceutical design


Optimization


Sensing and measuring


Secure communication


New innovations

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?**

Execution is

90% Planning

10% Doing

— Kathleen Taylor, Chair of the Board, RBC

Classical Paradigm

Encrypting and authenticating is easy (e.g. multiplying numbers)

Code breaking (e.g. factoring large numbers) is hard

Quantum Paradigm

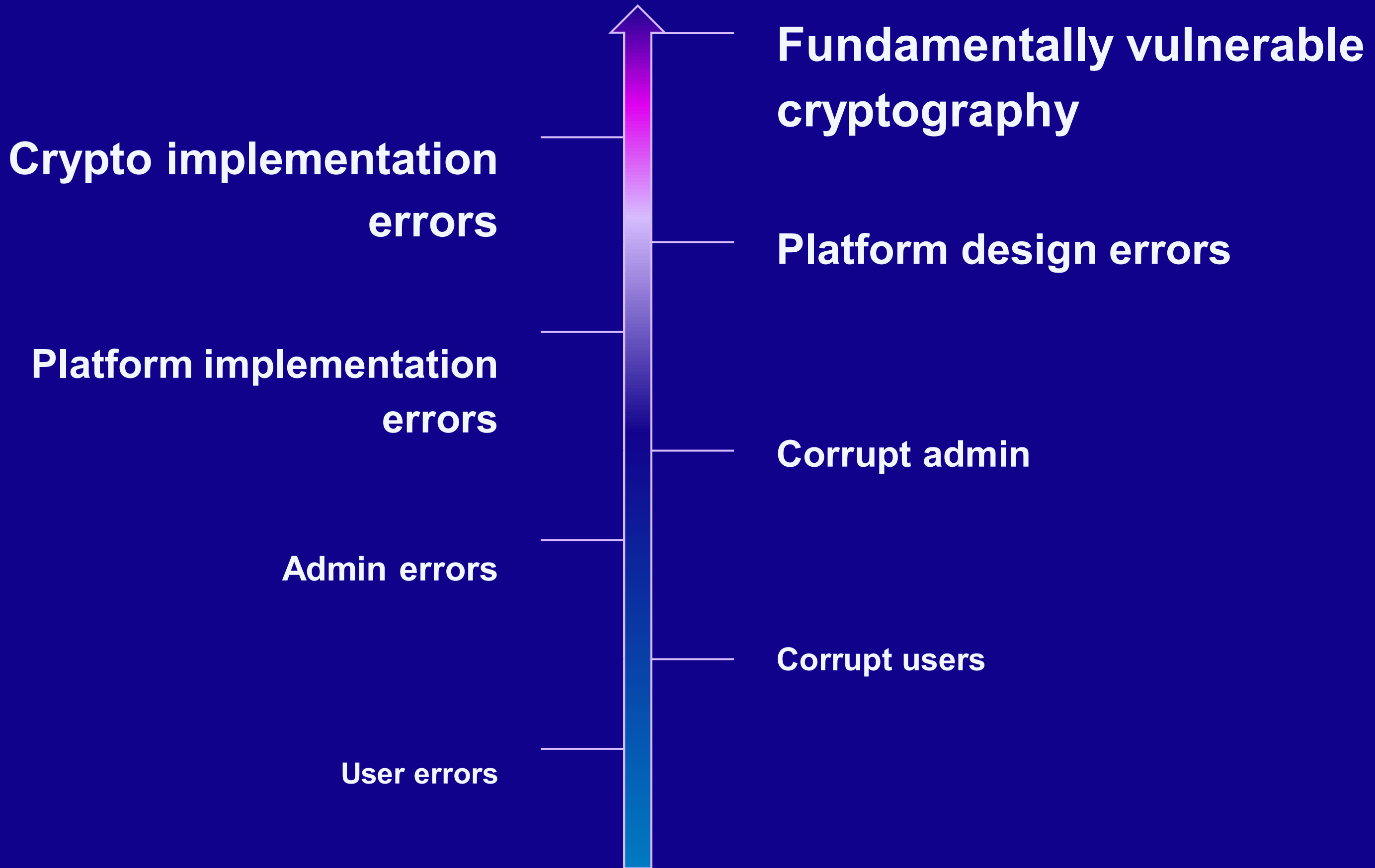
Encrypting and authenticating is easy

Breaking today's public key cryptography (i.e. factoring large numbers, finding discrete logarithms) is EASY

Vulnerabilities are exploited in many ways

- (D)DOS
- Ransomware
- Spyware
- Identify theft
- Cryptojacking
- Stolen data
- Data leaks
- Shutdown of infrastructure
- Etc.

Vulnerabilities, from bad to worse



When do we need to start?

As you plan your migration to quantum-safe protocols, consider:

Security shelf-life (x years)
Migration time (y years)
Collapse time (z years)

Migration time	Security shelf-life
Collapse time	

If x+y approaches z, act now!

Plan for security and resilience

Challenge		Mitigation
Critical infrastructure may fail and no quick fix exists	→	Make sure y<z
Data must remain confidential over time (record now, decrypt later)	→	Make sure x+y<z
Rushed preparations are expensive, disruptive, vulnerable to mistakes	→	Avoid the need to compress y; All of the above
Society could lose trust in tools and institutions underpinning our digital economy	→	All of the above
Quantum computing potential is restricted due to risk	→	All of the above
Upgraded algorithms protecting critical systems can be broken mathematically	→	Agility, defense-in-depth, methods not susceptible to cryptanalysis

Our luck may run out

The cryptographic “breaks” in the modern era have generally

- not been feasible in the short term (so there was time to react), or
- not been on widely deployed algorithms.

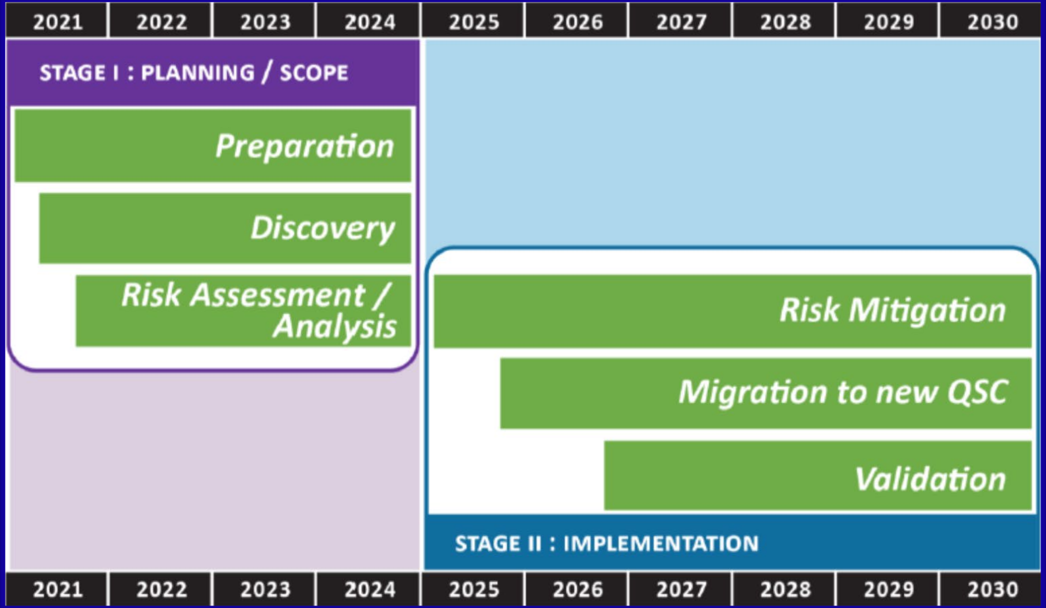
The stakes have grown astronomically, and continue to grow.

QRA Methodology

- **Phase 1:** Document current cryptographic protection
- **Phase 2:** Research and estimate timelines for both quantum computers and quantum-safe cryptography
- **Phase 3:** Estimate collapse time, “z”
- **Phase 4:** Identify asset lifetime, “x”, and quantum-safe transformation time, “y”
- **Phase 5:** Calculate quantum risk,
    - (x + y > z ?)
- **Phase 6:** Prioritize you quantum-safe migration steps

CFDIR Quantum Safe Journey

Quantum Readiness Program Timeline



CFDIR - Canadian National Quantum-Readiness:
Best Practices and Guidelines

Must also Prepare Future Platforms and Tools

Forbes

INNOVATION

Practical Homomorphic Encryption: Three Business Use Cases

Forbes Technology Council

Ellison Anne Williams Forbes Councils Member
Forbes Technology Council
COUNCIL POST | Membership (Fee-based)

Aug 10, 2020, 08:50am EDT

QUANTUM-PROOFING THE BLOCKCHAIN

Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, and Bill Munson

University of Waterloo

November 2017

A BLOCKCHAIN RESEARCH INSTITUTE BIG IDEA WHITEPAPER


In collaboration with Deloitte
WORLD ECONOMIC FORUM
Transitioning to a Quantum-Secure Economy
WHITE PAPER
SEPTEMBER 2022

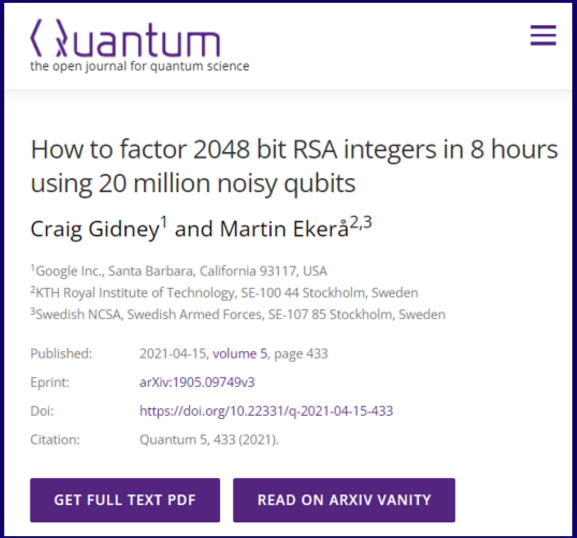
Collapse Time Impacted by:

- best known algorithms for breaking today's public key cryptography
- best known optimizations to these algorithms, including optimizations customized to specific architectures
- architecture details of quantum computing platforms (like connectivity)
- best known fault-tolerant quantum error correction
- currently available tools and their performance benchmarks, like error rates

Migration time	Security shelf-life
Collapse time	

Example of Progress

Using state-of-the-art "conventional" surface-code methods, with reasonable assumptions


the open journal for quantum science

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

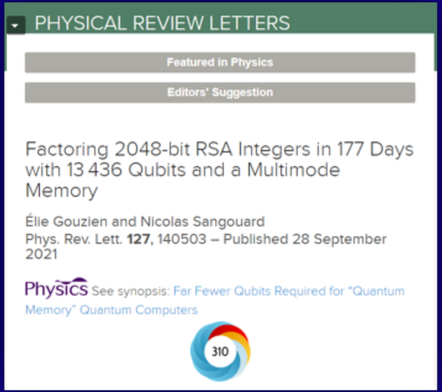
Craig Gidney[1] and Martin Ekerå[2,3]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[3]Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

Published:	2021-04-15, volume 5, page 433
Eprint:	arXiv:1905.09749v3
Doi:	https://doi.org/10.22331/q-2021-04-15-433
Citation:	Quantum 5, 433 (2021).

GET FULL TEXT PDF READ ON ARXIV VANITY

Less "conventional" alternatives


PHYSICAL REVIEW LETTERS

Featured in Physics

Editors' Suggestion

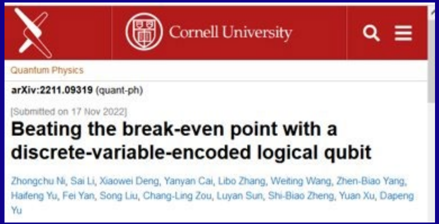
Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory

Élie Gouzien and Nicolas Sangouard

Phys. Rev. Lett. **127**, 140503 – Published 28 September 2021

Physics See synopsis: Far Fewer Qubits Required for "Quantum Memory" Quantum Computers

310


Cornell University

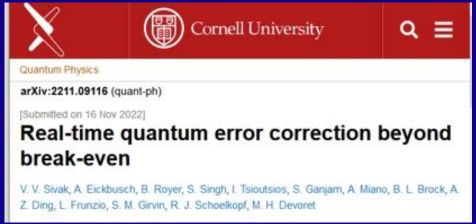
Quantum Physics

arXiv:2211.09319 (quant-ph)

[Submitted on 17 Nov 2022]

Beating the break-even point with a discrete-variable-encoded logical qubit

Zhongchu Ni, Sai Li, Xiaowei Deng, Yanyan Cai, Libo Zhang, Weiting Wang, Zhen-Biao Yang, Haifeng Yu, Fei Yan, Song Liu, Chang-Ling Zou, Luyan Sun, Shi-Biao Zheng, Yuan Xu, Dapeng Yu


Cornell University

Quantum Physics

arXiv:2211.09116 (quant-ph)

[Submitted on 16 Nov 2022]

Real-time quantum error correction beyond break-even

V. V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, A. Miano, B. L. Brock, A. Z. Ding, L. Frunzio, S. M. Girvin, R. J. Schoelkopf, M. H. Devoret

Breaking RSA with near-term devices??

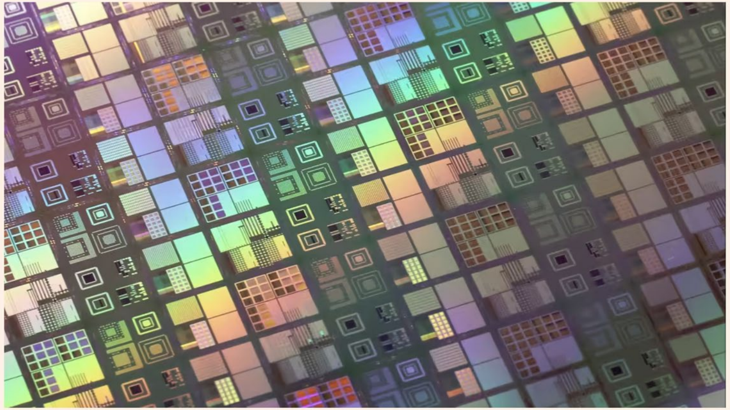
FINANCIAL TIMES

COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Quantum technologies + Add to myFT

Chinese researchers claim to find way to break encryption using quantum computers

Experts assess whether method outlined in scientific paper could be a sooner-than-expected turning point in the technology



A silicon wafer of quantum computer chips made by Hitachi © Yoshio Tsunoda/AFLO

https://www.ft.com/content/b15680c0-cf31-448d-9eb6-b30426c29b8b

nature

Explore content About the journal Publish with us Subscribe

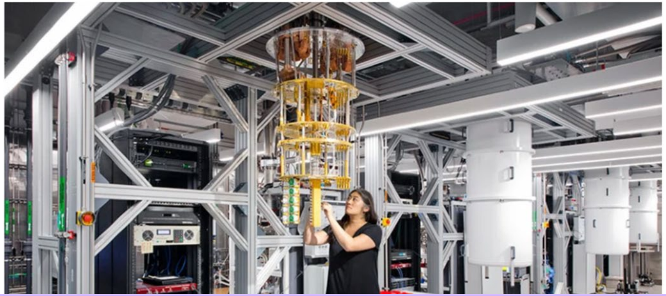
nature > news > article

NEWS | 06 January 2023

Are quantum computers about to break online privacy?

A new algorithm is probably not efficient enough to crack current encryption keys – but that's no reason for complacency, researchers say.

Davide Castelvecchi



https://www.nature.com/articles/d41586-023-00017-0

Status of Quantum Computer Development

Bundesamt
für Sicherheit in der
Informationstechnik

Studie: Entwicklungsstand
Quantencomputer V1.2

Datum 18.08.2020

Next Major Milestone:

Fault-Tolerant Logical Qubits

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

David Nield · 9/17/2020

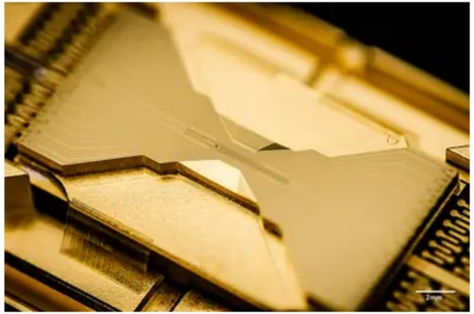
We're still a long way from realising the full potential of quantum computing, but scientists are making progress all the time – and as a sign of what might be coming, IBM now says it expects to have a 1,000 qubit machine up and running by 2023.

© IBM

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

TECHNOLOGY 1 October 2020

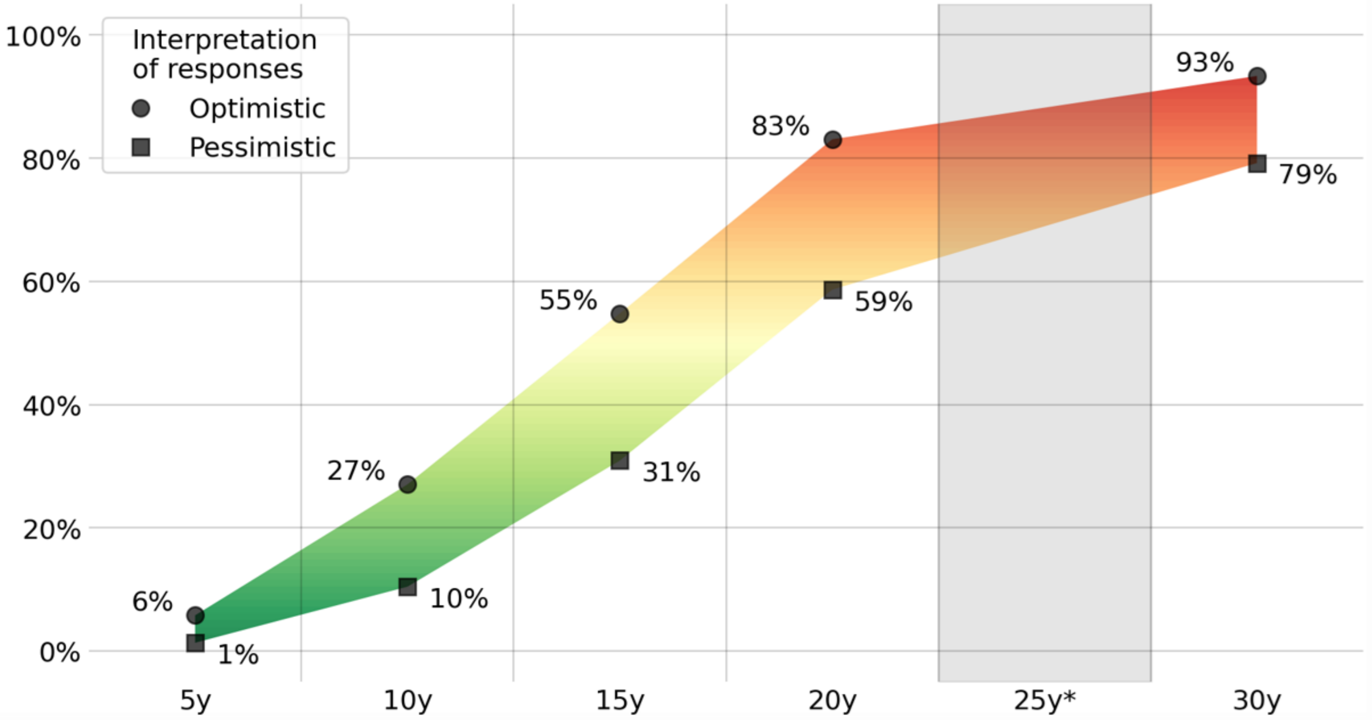
By Leah Crane



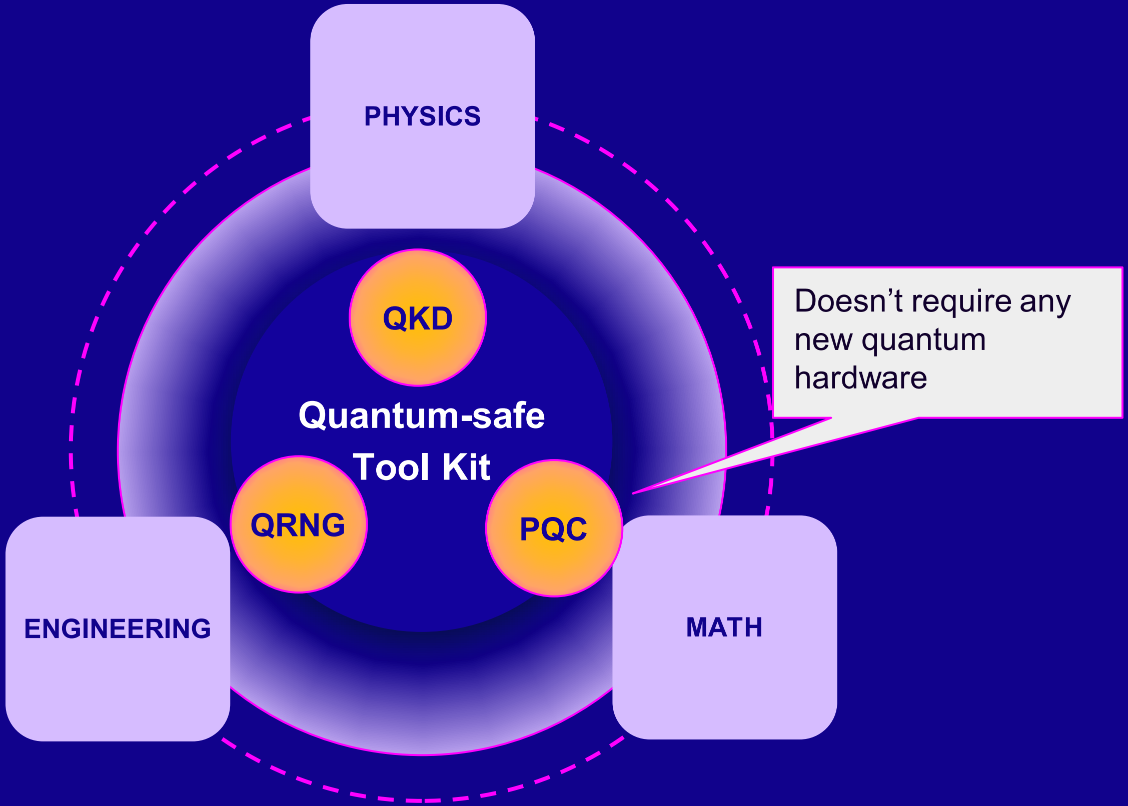
The ion trap at the heart of IonQ's quantum computer
Kai Hudek, IonQ

2022 OPINION-BASED ESTIMATES OF THE CUMULATIVE PROBABILITY OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIMEFRAME

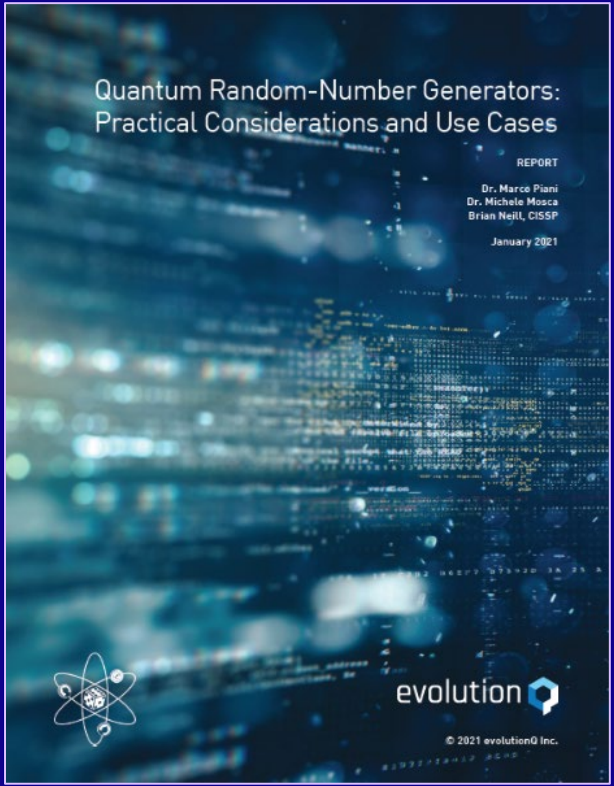
Estimates of the cumulative probability of a cryptographically-relevant quantum computer in time: range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the estimates indicated by the respondents.
[*Shaded grey area corresponds to the 25-year period, not considered in the questionnaire.]



Tools:
"Post-quantum" and quantum cryptography



True Randomness

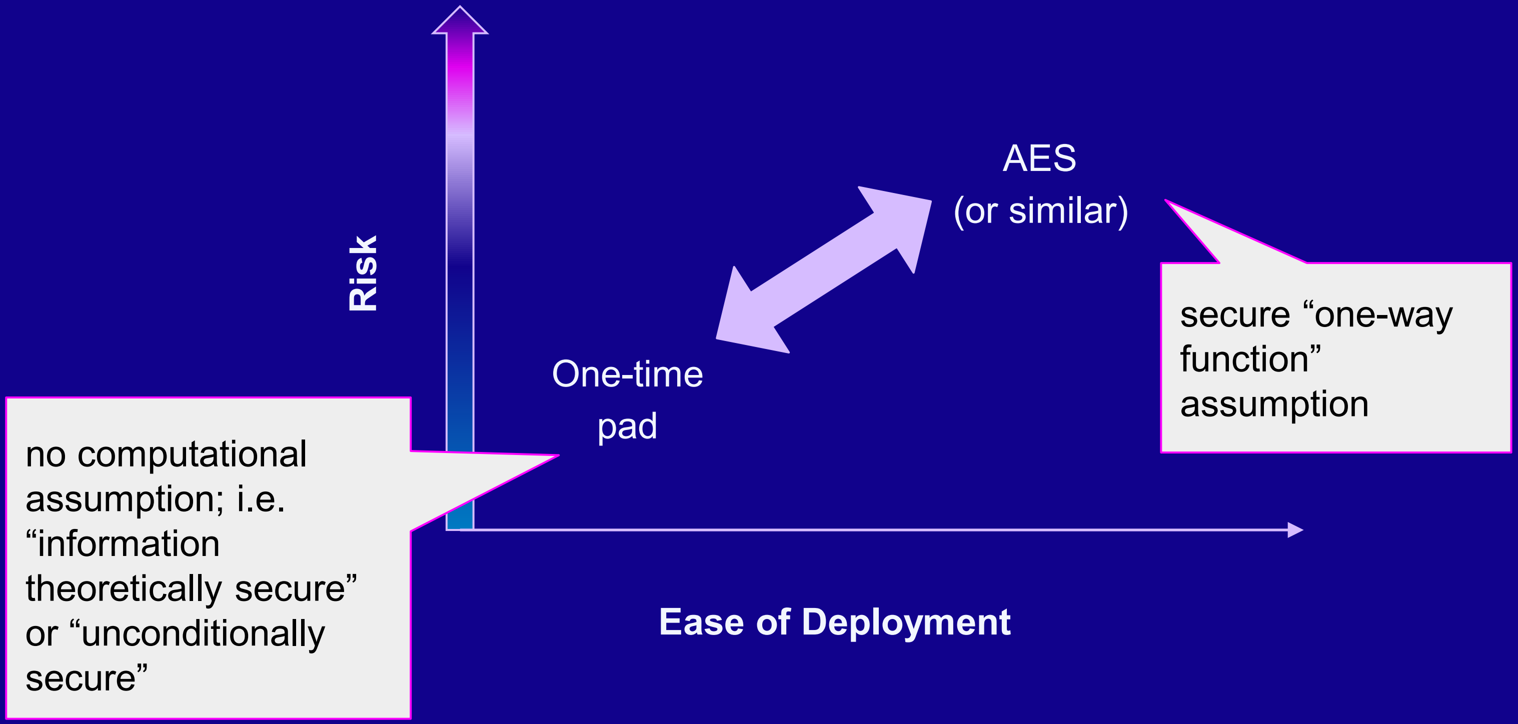


https://evolutionq.com/qrng-report-2021.html

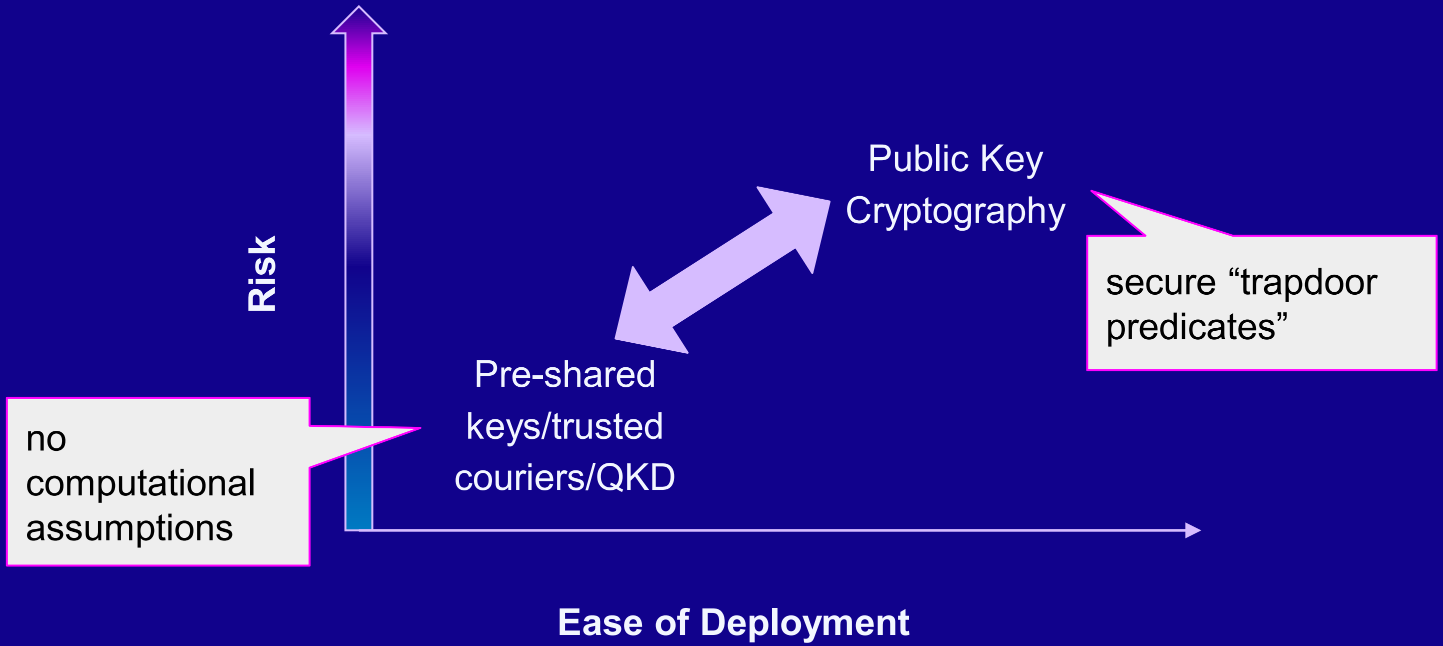
New quantum feature: Eavesdropper detectability

Enables key establishment without a computational assumpion. Known as Quantum Key Distribution (QKD).

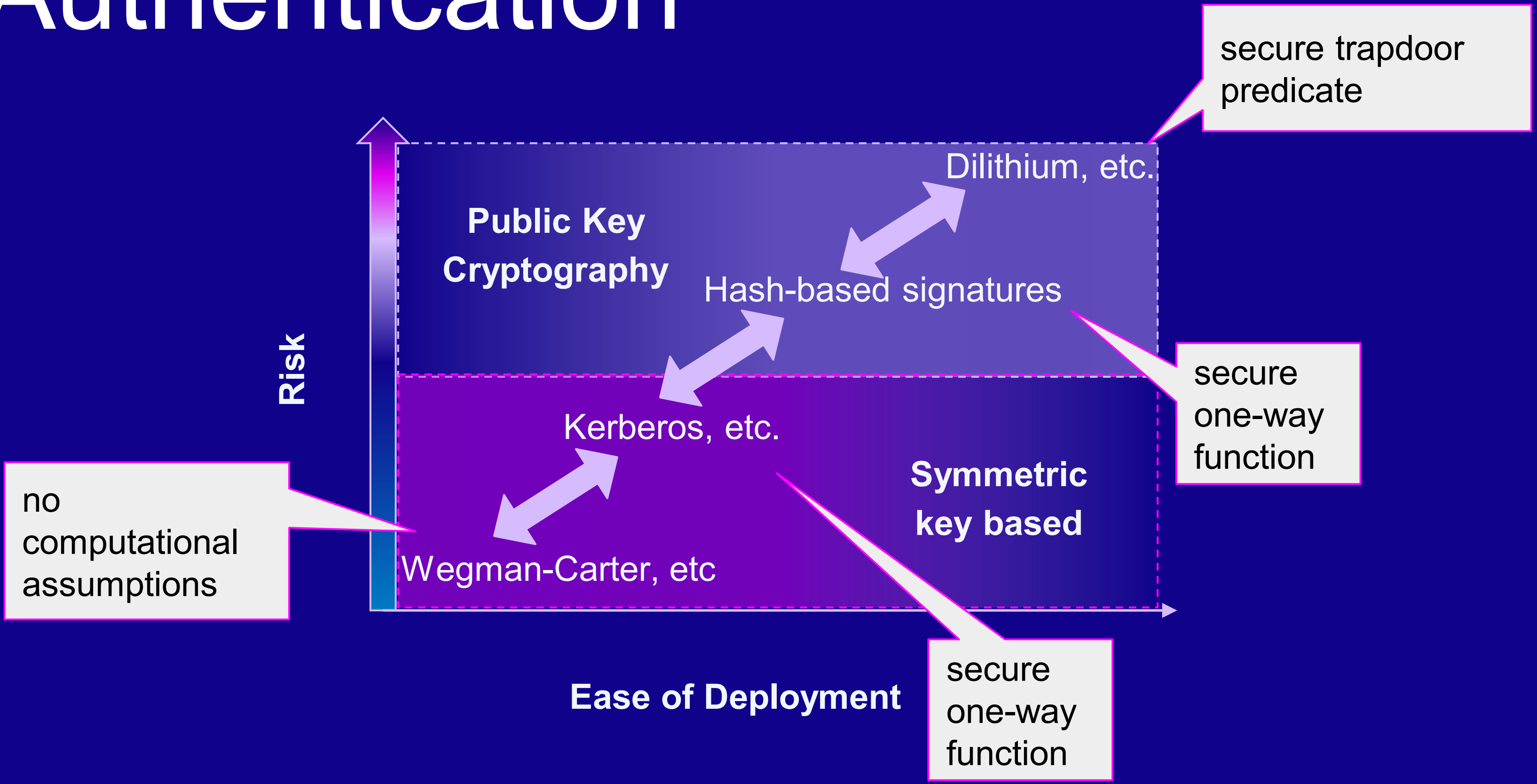
Symmetric Encryption



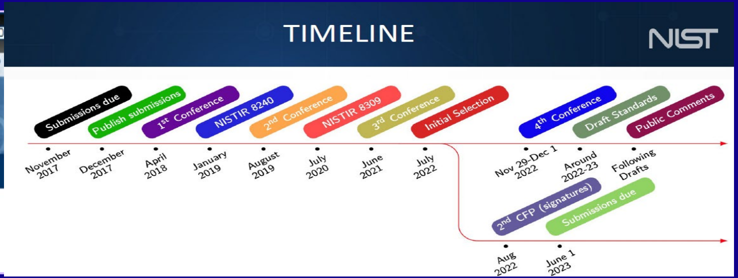
Key Establishment



Authentication



Ongoing Work to Develop Standards and Certifications for These Tools



Call to Action

- Establish quantum-readiness team within your organization with broad executive support.
- Leverage available “best practices” and contribute new findings back to the community.
- Support the vendor ecosystem we will all rely on. Testing solutions. Deploying sooner where risk equation calls for it.
- Engage with broader ecosystem (supply chain, third parties, standards, etc.) to identify key challenges that need to be tackled together.

Thank You!

Comments, questions and feedback are very welcome.

Michele Mosca
Professor, Faculty of Mathematics
Co-Founder, Institute for Quantum Computing,
University of Waterloo www.iqc.ca/~mmosca
mmosca@uwaterloo.ca

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

Co-founder, softwareQ Inc. softwareq.ca

Cybersecurity Risk

WORLD ECONOMIC FORUM

The World Economic Forum cites **cybercrime and cyber insecurity** as one of the top 10 global Risks in both the short and long-term.

2 years

1	Cost-of-living crisis
2	Natural disasters and extreme weather events
3	Geoeconomic confrontation
4	Failure to mitigate climate change
5	Erosion of social cohesion and societal polarization
6	Large-scale environmental damage incidents
7	Failure of climate change adaptation
8	Widespread cybercrime and cyber insecurity
9	Natural resource crises
10	Large-scale involuntary migration

10 years

1	Failure to mitigate climate change
2	Failure of climate-change adaptation
3	Natural disasters and extreme weather events
4	Biodiversity loss and ecosystem collapse
5	Large-scale involuntary migration
6	Natural resource crises
7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity
9	Geoeconomic confrontation
10	Large-scale environmental damage incidents