Prosperity and Resilience in the Quantum Era

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

evolution

Cybersecurity Risk

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

evolution

How can we entrust information and tasks to untrusted systems?

evolution

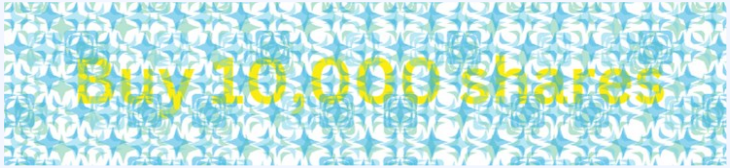
Quantum Changes What is “Secure”

Message, M

Buy 10,000 shares

Encryption Key, k

CipherText, (k,M)



Decryption Key, k

Decrypted Message, M

Buy 10,000 shares

evolution

Quantum Changes Everything

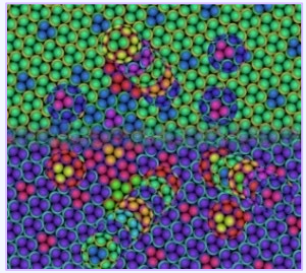
Key Establishment

Symmetric Encryption

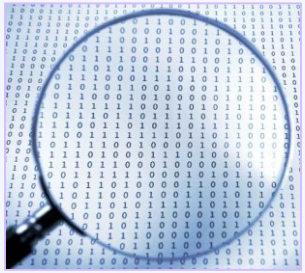
Authentication

evolution

Quantum Brings Immense Power



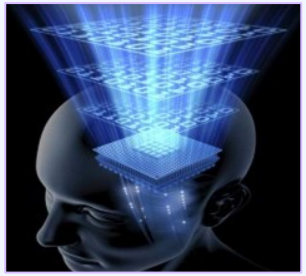
Material and pharmaceutical design



Optimization

Secure communication

Sensing and measuring



New innovations

evolution

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?**

evolution

Execution is
90% Planning
10% Doing

— Kathleen Taylor, Chair of the Board, Royal Bank of Canada

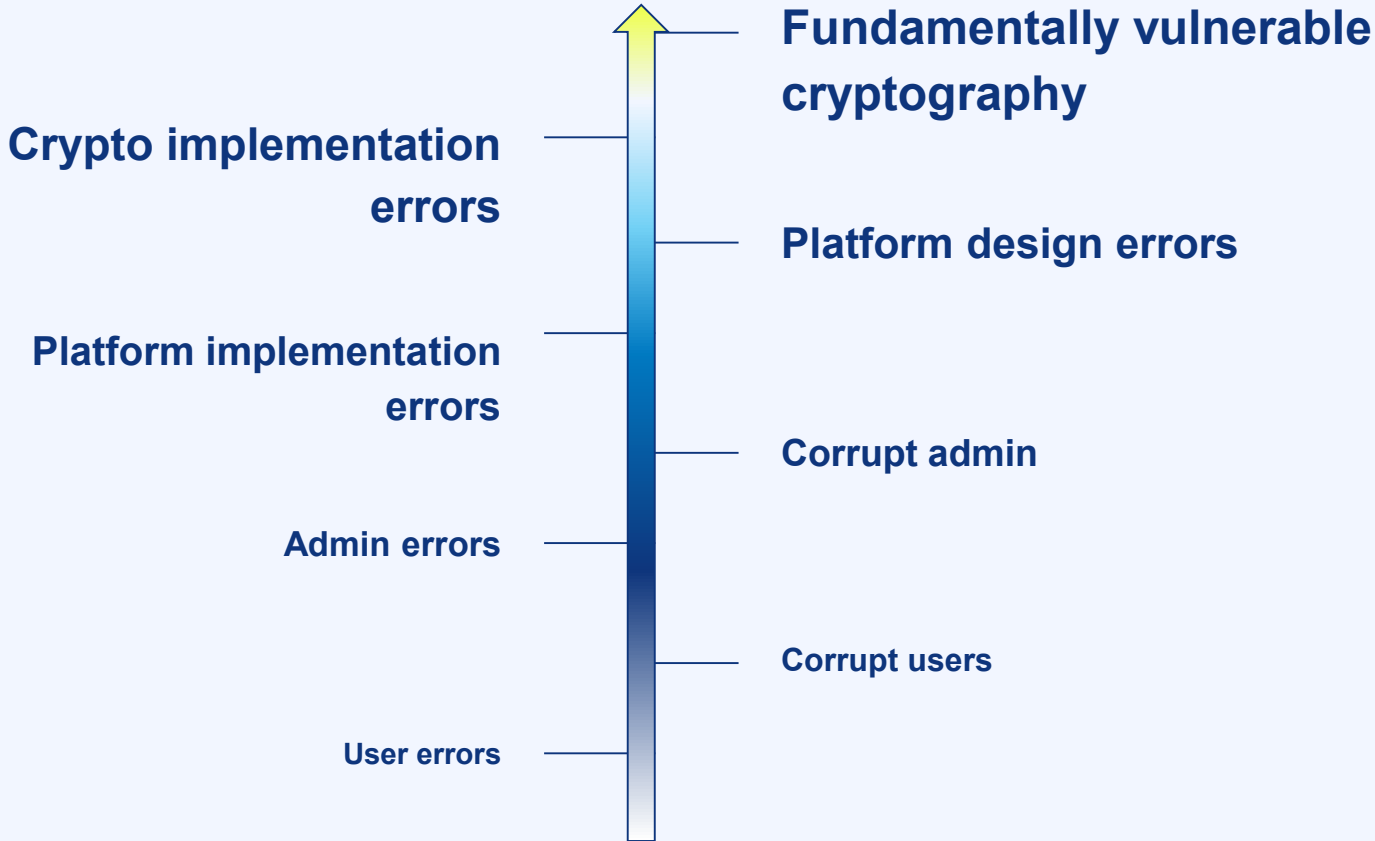
evolution

Vulnerabilities are Exploited in Many Ways

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

evolution

Vulnerabilities, from Bad to Worse



evolution

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)

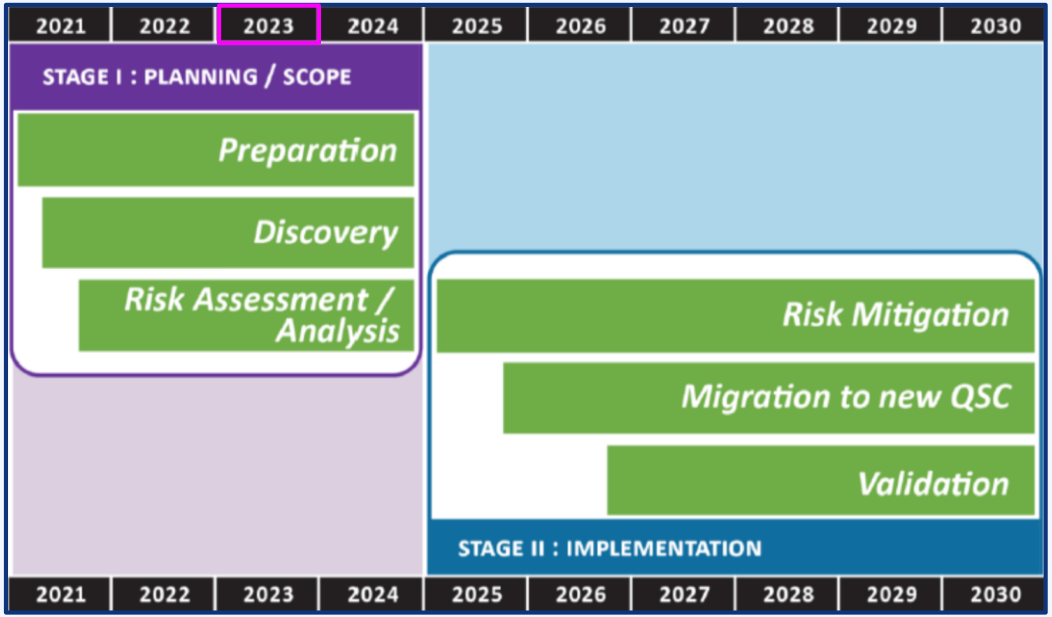
The Mosca Equation

If x+y approaches z, act now!

evolution

CFDIR Quantum Safe Journey

Quantum Readiness Program Timeline

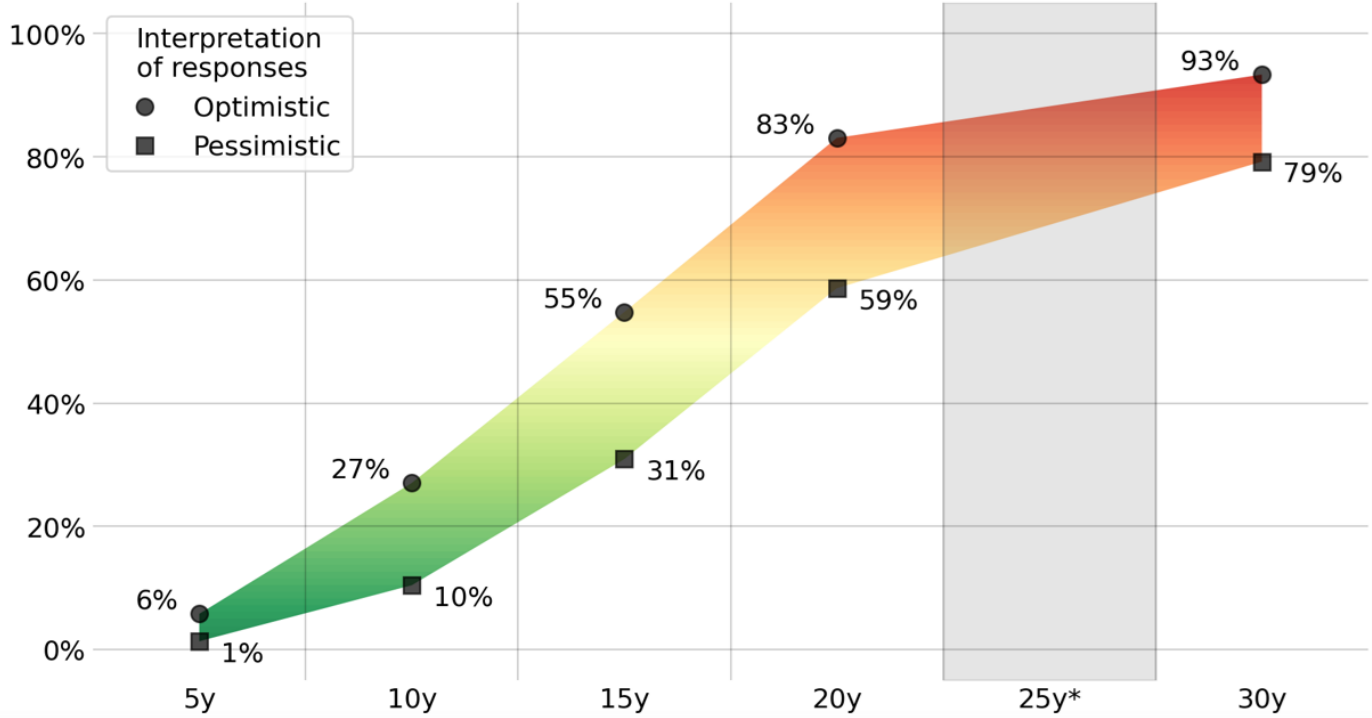


CFDIR - Canadian National Quantum-Readiness:
Best Practices and Guidelines

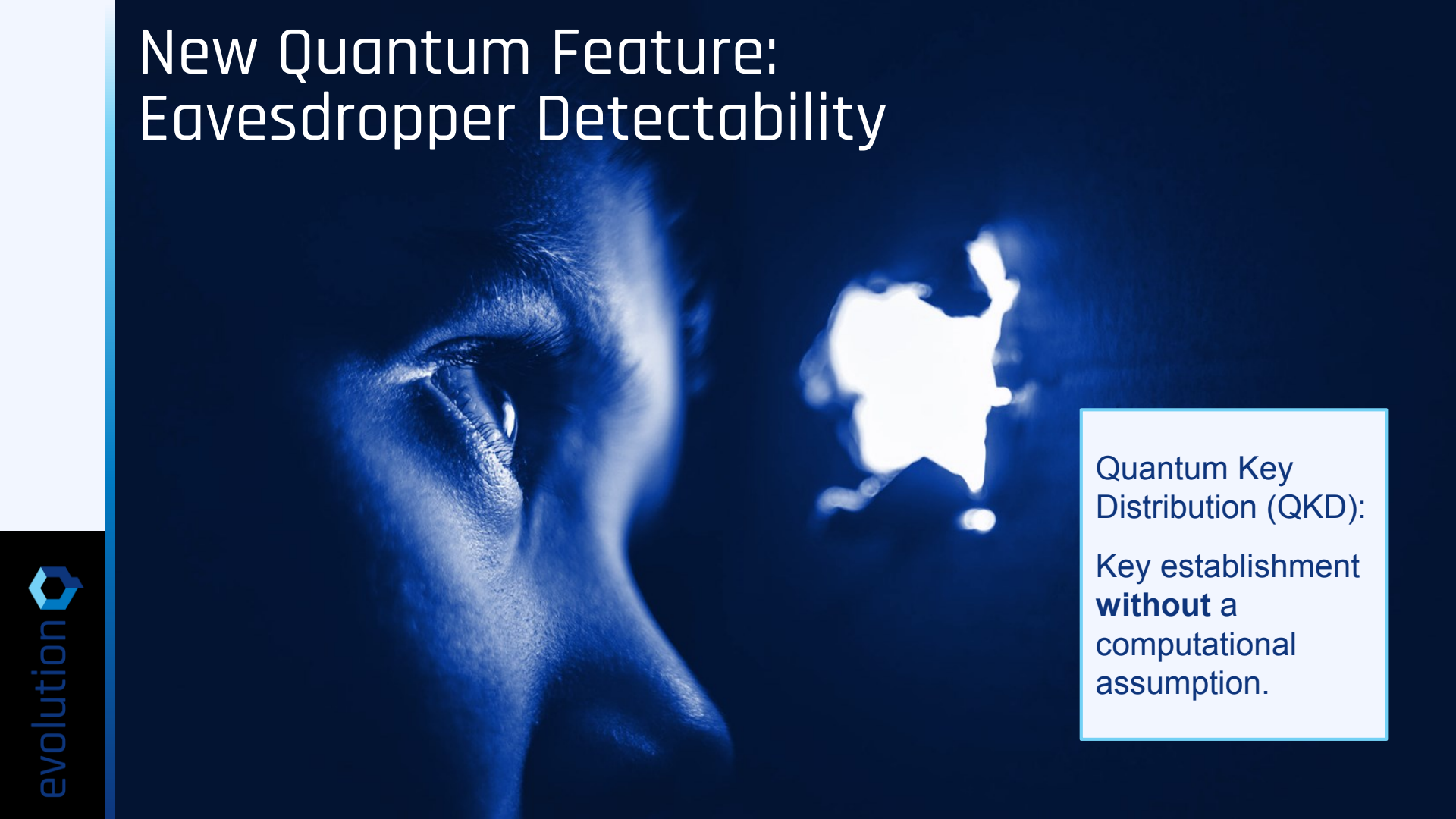
evolution

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.]



New Quantum Feature: Eavesdropper Detectability

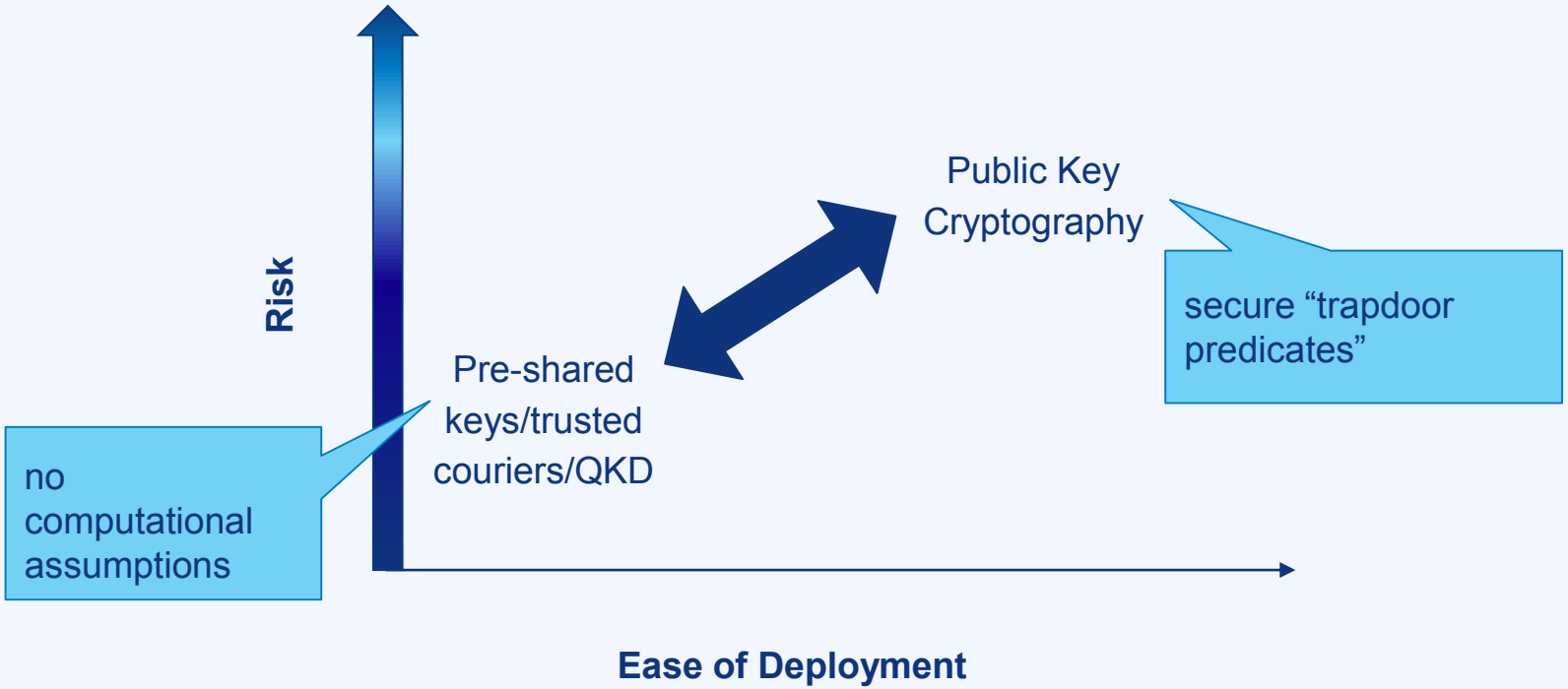


Quantum Key Distribution (QKD):

Key establishment **without** a computational assumption.

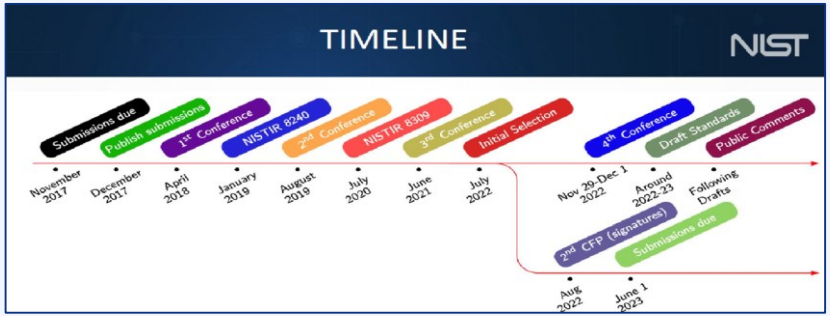
evolution

Key Establishment



evolution

Ongoing Work to Develop Standards and Certifications for These Tools



evolution

You Can Start Today

- Maximize India's ROI in quantum innovation
  - Establish quantum readiness requirements for key economic sectors
  - Leverage available "best practices" and contribute new findings back to the community
- Support the vendor ecosystem we will all rely on
  - Test solutions in real-world scenarios
  - Deploy when indicated by the risk equation
- Engage with broader ecosystem (supply chain, third parties, standards, etc.) to identify key challenges that need to be tackled together

evolution

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

evolution