

Cybersecurity in an era with quantum computers: will we be ready?

Michele Mosca
19 October 2016

CryptoWorks21



UNIVERSITY OF
WATERLOO

IQC

Institute for
Quantum
Computing

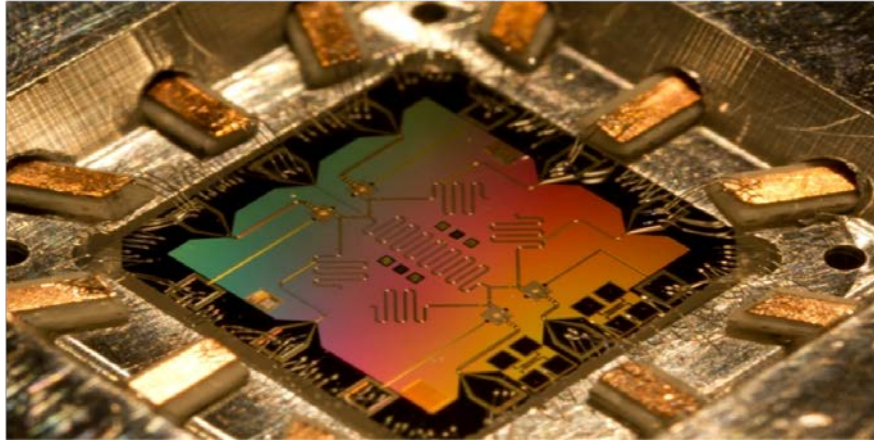
evolution 

PERIMETER  INSTITUTE FOR THEORETICAL PHYSICS

A new paradigm for physics: quantum mechanics



A new paradigm for computation: quantum computation

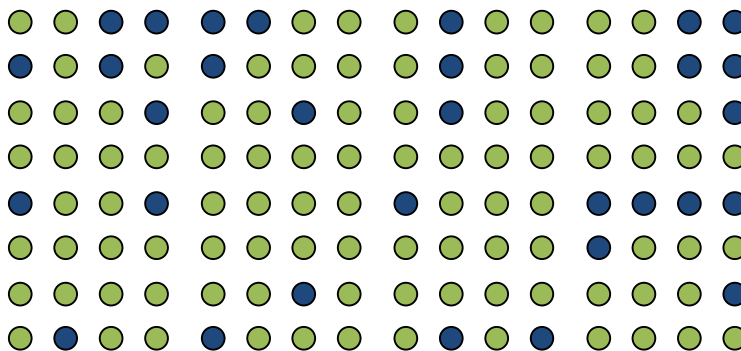
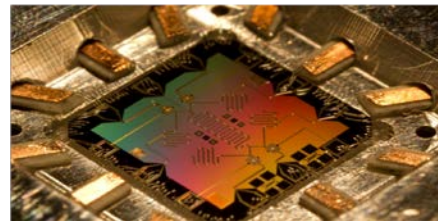


E. Lucero, D. Mariani, and M. Mariani

What is a quantum computer?

- What is a classical computer?
- A device that encodes information in an array of bits, and can manipulate those bits according to simple rules.

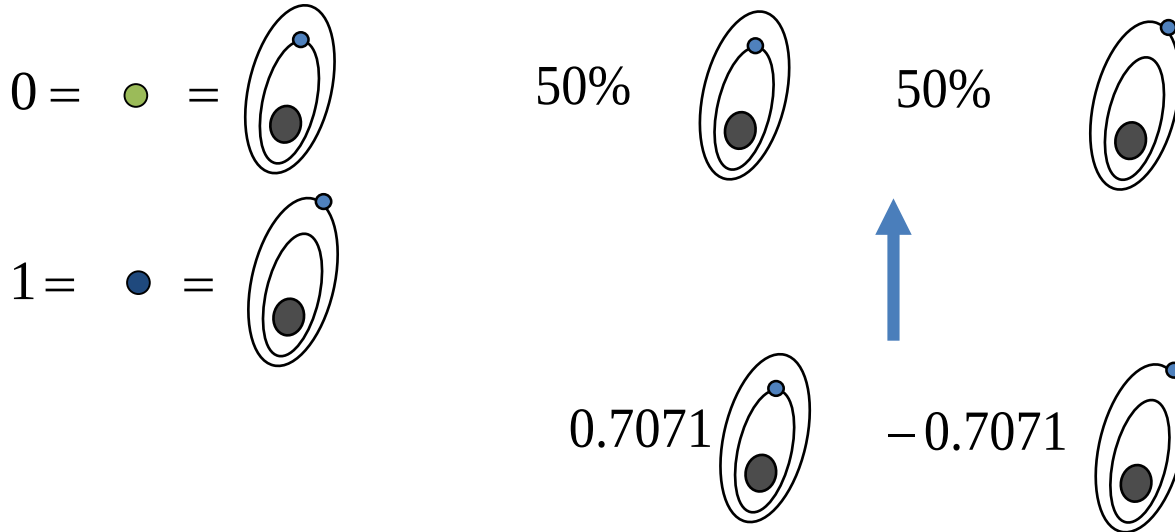
● = 0 ● = 1



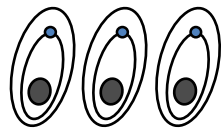
"I've always wanted to peek under the hood of one of these bad boys."

New feature: superposition/parallelism

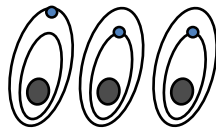
A physical system that can exist in two or more distinguishable states can in a special way embody all the distinguishable states at the same time



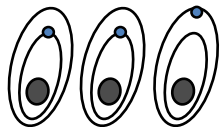
0.121



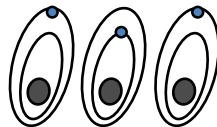
- 0.875



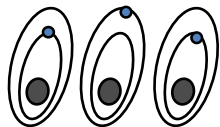
-0.242



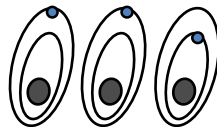
+0.000



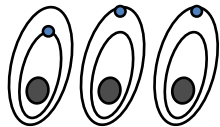
+0.000



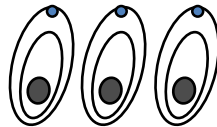
+0.000



- 0.019



+ 0.401



Simulating quantum bits with classical bits

- Describing n qubits in a classical computer in this way uses more than 2^n bits of memory.

# 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	$340282366920938463463374607431768211456=2^{128}$ ~ 3.4×10^{38}
230	$1725436586697640946858688965569256363112777243042596638790631055949824=2^{230}$ ~ 10^{100}

What are quantum computers good for?

"Global" patterns: Seeing the forest without observing the trees.

Example:

The sequence 34, 12, 54, 38, 57, 34, 12, 54, 38, 57, 34, 12, ... has a *period* of length 5.

Imagine a sequence with an astronomically large period.

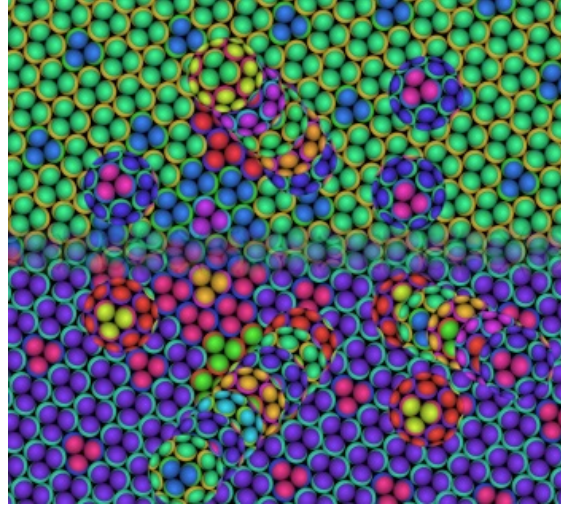
Example

With a handful of quantum glimpses:

"length of period = 729672482463"

"any specific value in the sequence = ???"

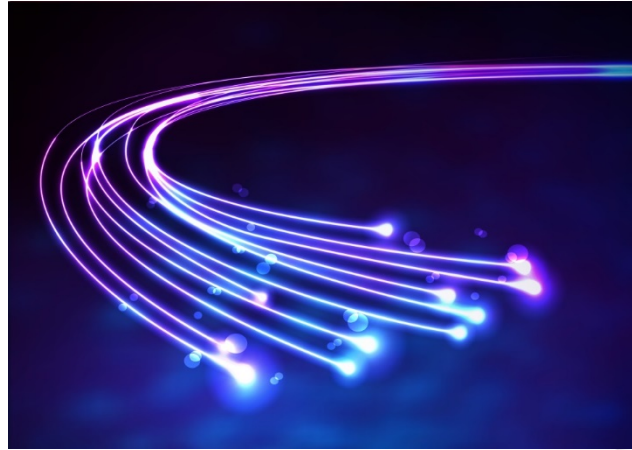
Applications: studying materials and chemicals



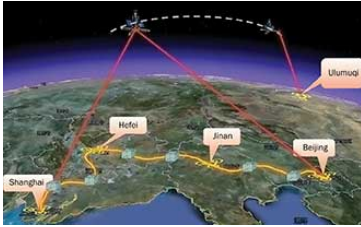
Applications: Searching and Optimizing



New feature: Eavesdropper detection



Quantum Cryptography



Courtesy of Qiang Zhang, USTC

Beijing-
Shanghai
QKD Backbone



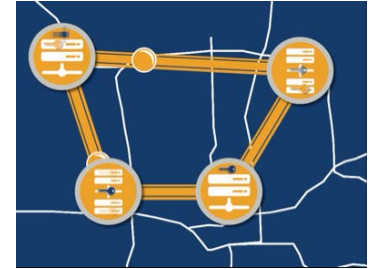
swissquantum.idquantique.com/?-Network-

SwissQuantum
Network



<http://www.uqcc.org/QKDnetwork/>

Tokyo QKD
Network



<http://www.battelle.org/our-work/national-security/cyber-innovations/quantum-key-distribution>

Battelle QKD
Network
Columbus, Ohio,
USA



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



<http://www.quantum-comm.com/index.php/Cate/index/pid/1>



<http://www.qasky.com/Product.aspx?id=94>

Free-space Quantum Cryptography



Thomas Jennewein et al., Smiths Falls, Ontario, Canada, Sept. 2016

THE WALL STREET JOURNAL.

Subscrib

SUBSC

[Home](#) [World](#) [U.S.](#) [Politics](#) [Economy](#) [Business](#) [Tech](#) [Markets](#) [Opinion](#) [Arts](#) [Life](#) [Real Estate](#)



🔑 [China Rethinks Its Alliance With Reeling Venezuela](#)



🔑 [Syria Rebels Press Fight Against Assad](#)



🔑 [Libyan Forces Loyal to Eastern Government Attack Key Oil Ports](#)



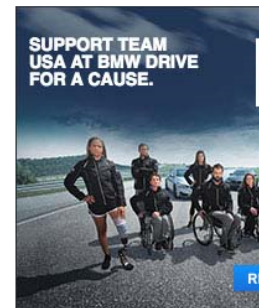
🔑 [New Tricks Make ISIS, Once Easily Tracked, a Sophisticated Opponent](#)



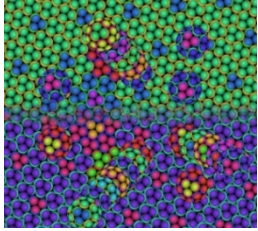
[WORLD](#) | [ASIA](#) | [CHINA NEWS](#)

China's Latest Leap Forward Isn't Just Great—It's Quantum

Beijing launches the world's first quantum-communications satellite into orbit



New paradigm brings new possibilities



Designing
new
materials,
drugs, etc.



Optimizing



Sensing and
measuring

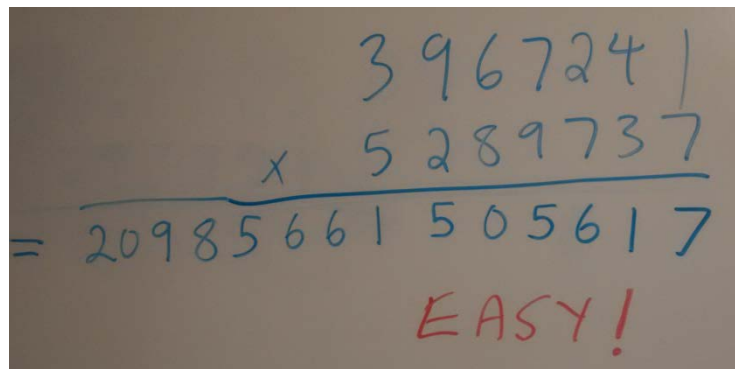


Secure
communication



What
else???

But... while in the old paradigm

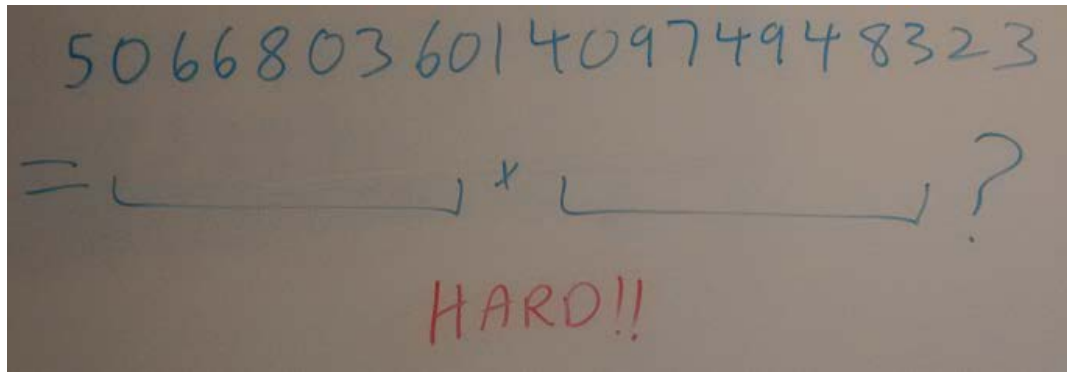


A handwritten multiplication problem on a piece of paper. The numbers are written in blue ink. The first number is 3967241, and the second number is 5289737. They are multiplied to get the result 20985661505617. The word "EASY!" is written in red ink below the result.

$$\begin{array}{r} 3967241 \\ \times 5289737 \\ \hline = 20985661505617 \end{array}$$

EASY!

Encrypting is easy.



A handwritten codebreaking problem on a piece of paper. The numbers are written in blue ink. The first number is 506680360140974948323. Below it is an equals sign followed by a bracketed space, a multiplication sign, another bracketed space, and a question mark. The word "HARD!!" is written in red ink below the question mark.

$$506680360140974948323 = \underline{\quad} \times \underline{\quad} ?$$

HARD!!

Codebreaking is hard.

...in the quantum paradigm



$$\begin{array}{r} 3967241 \\ \times 5289737 \\ \hline = 20985661505617 \end{array}$$

EASY!

Encrypting is easy.

$$\begin{array}{r} 506680360140974948323 \\ = \underbrace{13561998077} \times \underbrace{37360303199} ? \end{array}$$

EASY!!

Codebreaking is **easy**!

Cyber attacks

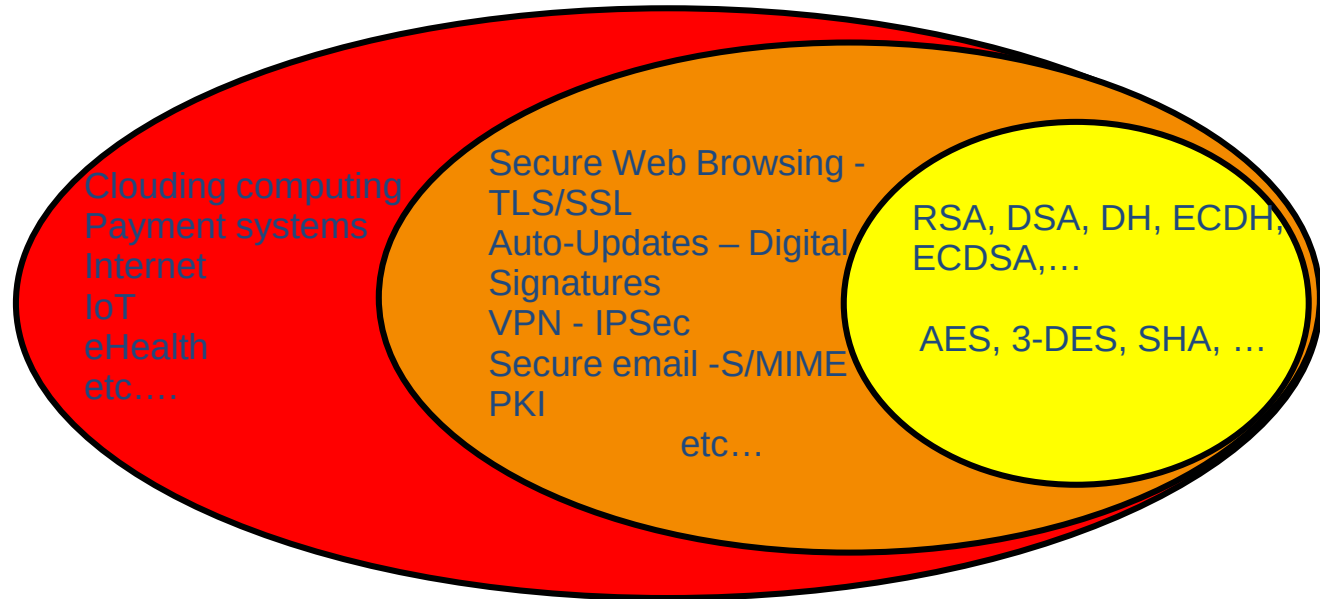


How secure will our current crypto algorithms be?

Algorithm	Key Length	Security level (Conventional Computer)	Security level (Quantum Computer)
RSA-1024	1024 bits	80 bits	~0 bits
RSA-2048	2048 bits	112 bits	~0 bits
ECC-256	256 bits	128 bits	~0 bits
ECC-384	384 bits	192 bits	~0 bits
AES-128	128 bits	128 bits	~64 bits
AES-256	256 bits	256 bits	~128 bits

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.

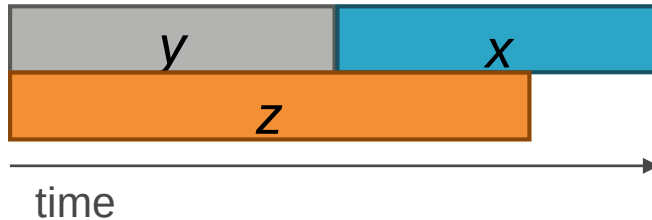


Do we need to worry *now*?

Depends on:

- $X = \text{security shelf-life}$
- $Y = \text{migration time}$
- $Z = \text{collapse time}$

“Theorem”: If $X + Y > Z$, then worry.



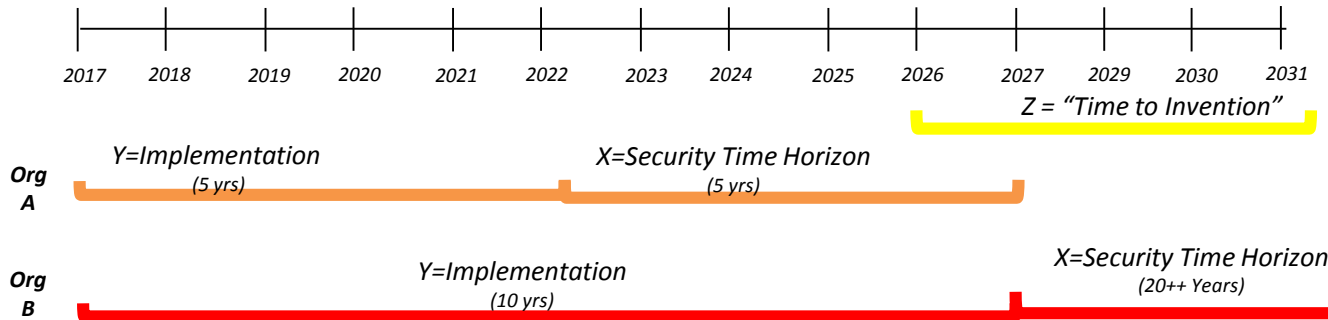
Why do we need to worry *now*?

- X = security shelf-life (required security time horizon)
- Y = migration time (planning and full implementation)
- Z = collapse time (time to development of quantum capability)



“Theorem”: If $X + Y > Z$, then worry.

Targeting existing encryption key systems → unlocks everything using legacy capabilities



Bottom line

Fact: If $X+Y>Z$, then you will not be able to provide the required X years of security.

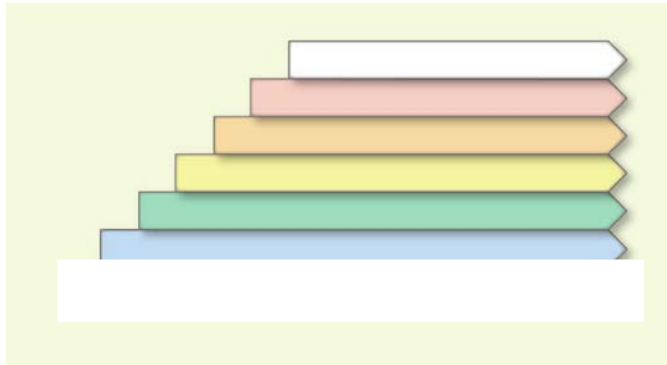
Fact: If $Y>Z$ then cyber systems will collapse in Z years with no quick fix.

Building a large quantum computer

REVIEW

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret^{1,2} and R. J. Schoelkopf^{1*}



SCIENCE VOL 339 8 MARCH 2013

Towards a fault-tolerant design

IARPA [July 2015]: *“BAA Summary – Build a logical qubit from a number of imperfect physical qubits by combining high-fidelity multi-qubit operations with extensible integration.”*

Several leading groups internationally have reported receiving awards.

What I don't worry about

- How big of a number has been quantumly factored to date [wrong benchmark]
- “Quantum computing” approaches that do not have a path for fault-tolerantly implementing quantum algorithms that are known to threaten cryptography (e.g. “adiabatic quantum computers”) [not a known threat]

What is 'z'?

Mosca:

[Oxford] 1996: *"20 qubits in 20 years"*

[NIST April 2015, ISACA September 2015]:

"1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031"

Microsoft Research [October 2015]: *Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer **within a decade**. ...Use of a quantum computer enables much larger and more accurate simulations than with any known classical algorithm, and will allow many open questions in quantum materials to be resolved once a small quantum computer with around **one hundred logical qubits** becomes available.*

Quantum-safe cryptographic tool-chest

**conventional quantum-safe
cryptography**

a.k.a. Quantum Resistant Algorithms
(QRA) or Post-Quantum Cryptography

- Deployable without quantum technologies
- Believed/hoped to be secure against quantum computer attacks of the future

+ **quantum cryptography**

- Requires some quantum technologies (less than a large-scale quantum computer)
- Typically no computational assumptions and thus known to be cryptographically secure against quantum attacks

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

Security is a choice





National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC:

GO

[CONTACT](#) [SITE MAP](#)

Computer Security Division

Computer Security Resource Center

[CSRC Home](#) [About](#) [Projects / Research](#) [Publications](#) [News & Events](#)

Post-Quantum Cryptography
Project ▶

[Documents](#)

[CSRC HOME](#) > [GROUPS](#) > [CT](#) > POST-QUANTUM CRYPTOGRAPHY PROJECT

POST-QUANTUM CRYPTO PROJECT

NEWS -- August 2, 2016: The National Institute of Standards and Technology

4th ETSI-IQC Workshop on Quantum-Safe Cryptography



The image is a screenshot of the ETSI (European Telecommunications Standards Institute) website. At the top left is the ETSI logo. To its right is a search bar with the placeholder text "Search...". Further right are two buttons: "Website" (highlighted in blue) and "Standards" (in green). Below these are five navigation tabs: "Standards", "Technologies & Clusters", "Membership", "News & Events", and "Com". The main content area features a large banner for the "WORKSHOP ON QUANTUM-SAFE CRYPTOGRAPHY". The banner has a blue background with a pattern of white and yellow text. On the left side of the banner, it says "SEPT 2016" and "19-21" in large white font. The title "WORKSHOP ON QUANTUM-SAFE CRYPTOGRAPHY" is in large white capital letters. At the bottom of the banner, it says "TORONTO (CA)" in smaller white capital letters. There are also small navigation arrows on the right side of the banner.

ETSI

Search...

Website Standards

Standards Technologies & Clusters Membership News & Events Com

SEPT 2016
19-21

**WORKSHOP ON
QUANTUM-SAFE
CRYPTOGRAPHY**

TORONTO (CA)



PREDICTIVE IS NIMBLE.
ENSURE UPTIME ALL THE TIME.



Prepare for threat of quantum computing to encrypted data, Canadian conference told

Howard Solomon - September 20, 2016

"I think we are already behind," Scott Jones, deputy chief of IT security at the Communications Security Establishment (CSE), responsible for securing federal information systems, told the [fourth annual international workshop on quantum-safe cryptography](#) in Toronto on Monday.

CANADIAN POLITICS

TRENDING [Blue Jays](#) | [Brangelina](#) | [Trump](#) | [Clinton](#) | [Real estate](#) | [World Cup of Hockey](#) | [Lotto Max](#)

Quantum computing will cripple encryption methods within decade, spy agency chief warns

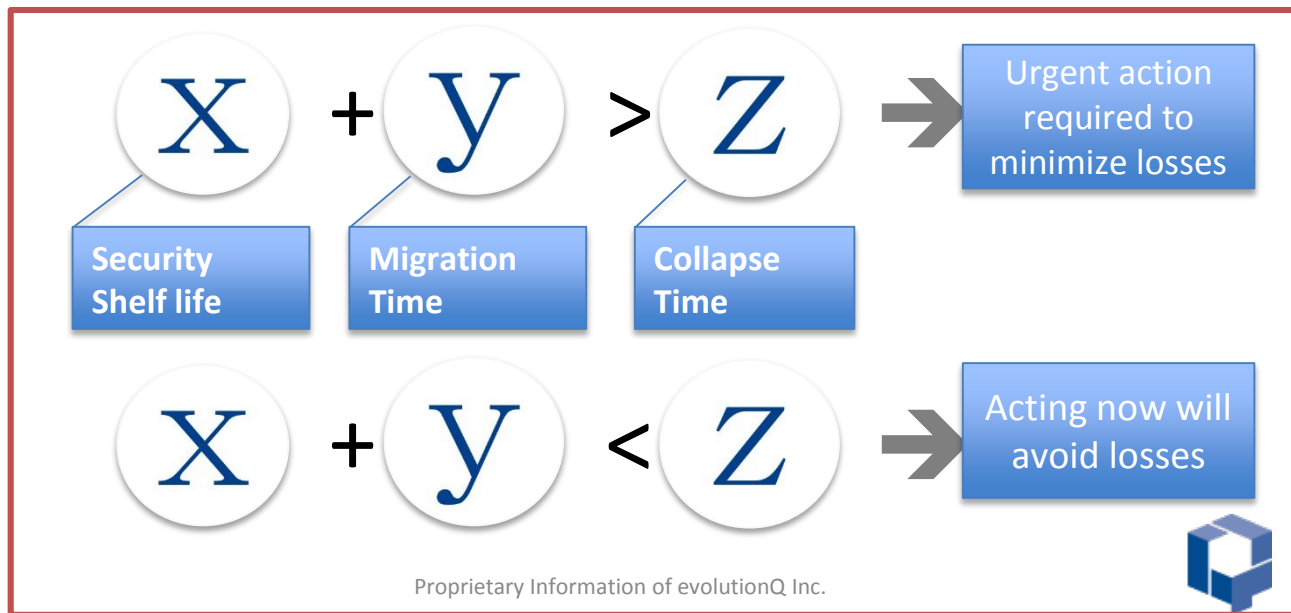


IAN MACLEOD, OTTAWA CITIZEN | September 23, 2016 7:54 PM ET
[More from Ian MacLeod, Ottawa Citizen](#)



Managing the quantum risk

- We need to assess x,y and z for the range of information assets and business functions.



Assessing and managing ‘y’

- This is the part we have control over
- Leverage existing risk mitigation policies, procedures, and processes.
- Manage community and technical challenges to deploying quantum-safe cryptography.
- Consider “hybrid” approaches to retain robustness of tools protecting against today’s threats while introducing new tools designed to protect against the future quantum threat.

openquantumsafe.org



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/~mmosca

Director, CryptoWorks21 www.cryptoworks21.com

University of Waterloo

mmosca@uwaterloo.ca

Co-founder and CEO

evolutionQ Inc. www.evolutionq.com

michele.mosca@evolutionq.com