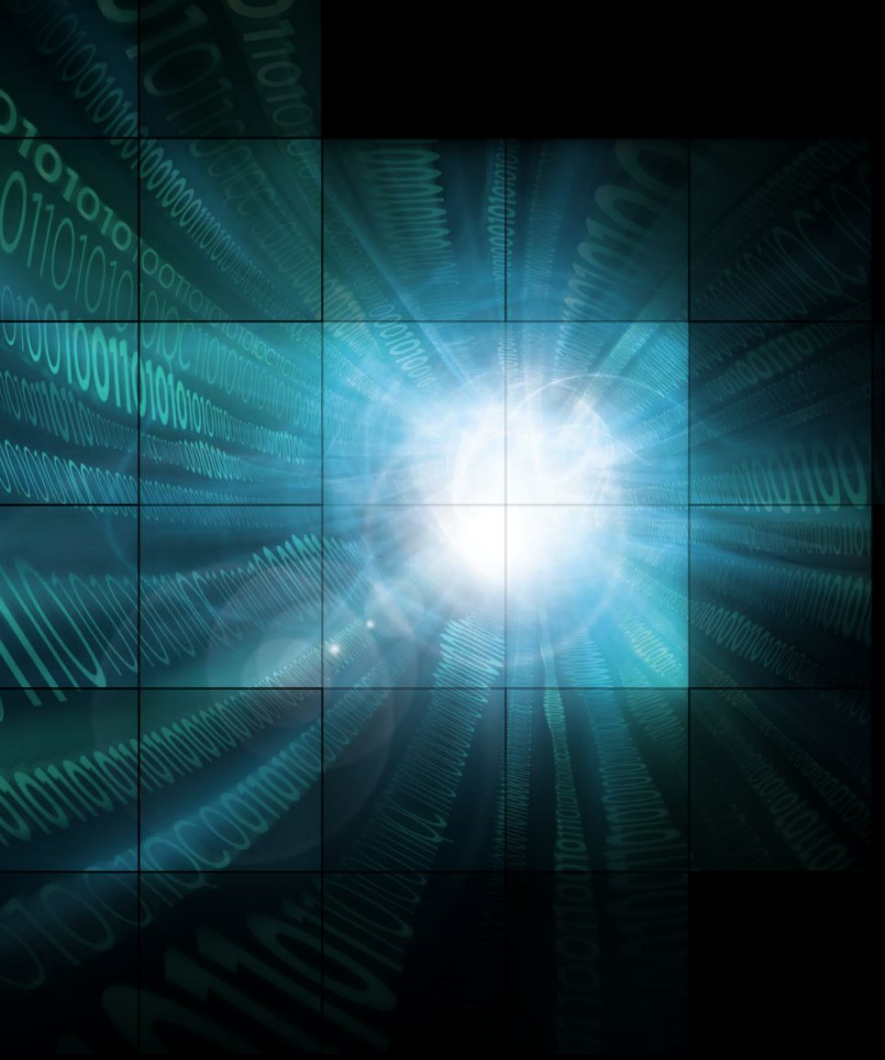


Update on the Quantum Threat, Mitigation, and Relevant Timelines

ICMC 2016
Ottawa

Michele Mosca
20 May 2016

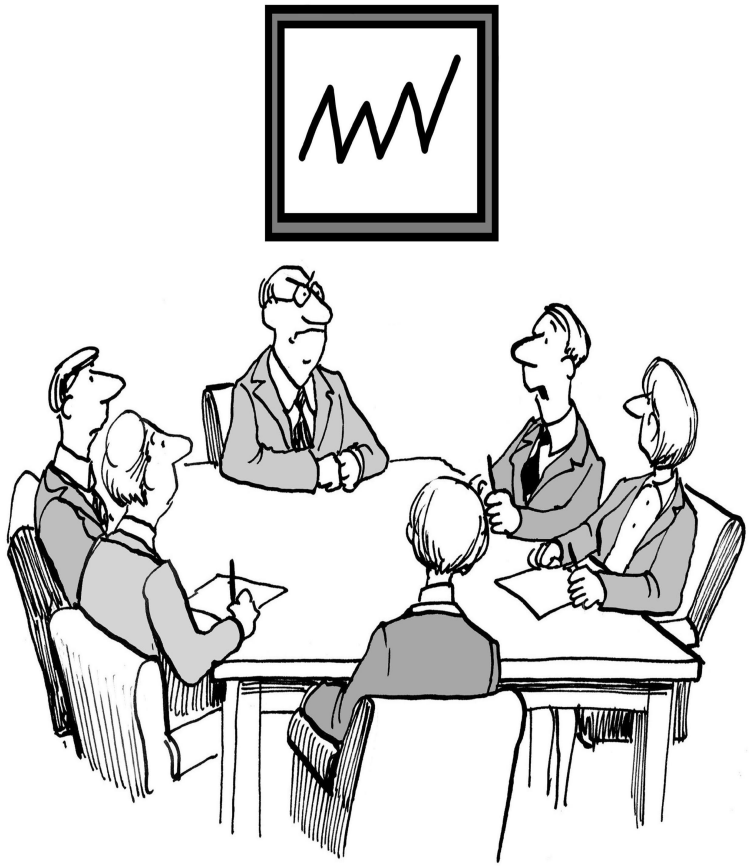
PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

evolutionQ

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

CryptoWorks21

Unpredictable new vulnerabilities

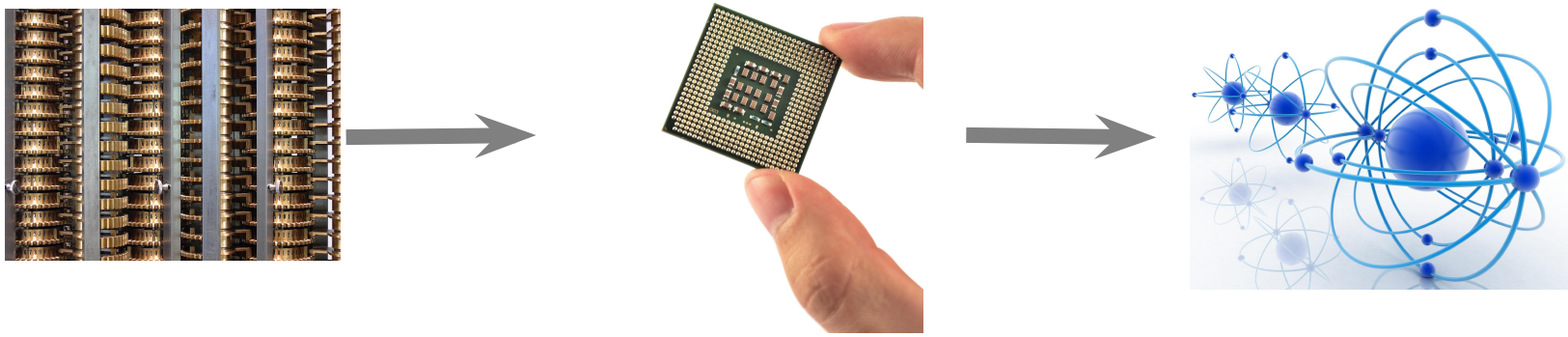


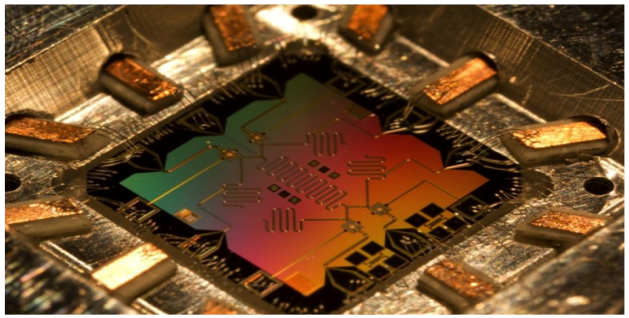
"As is the norm, an unexpected problem occurred today."

"going up a down escalator"

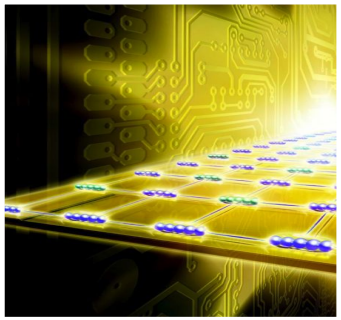
Physics and Computation

Information is physical … so we must recast information and computation in a quantum paradigm.

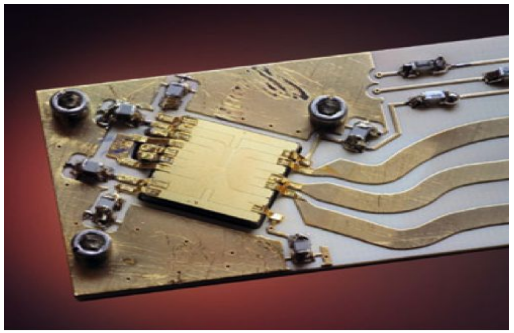




E. Lucero, D. Mariantoni, and M. Mariantoni



© Harald Ritsch



Y. Colombe/NIST

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Simulating quantum bits with classical bits

Describing *n* qubits in a classical computer uses more than 2^n bits 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	$340282366920938463463374607431768211456=2^{128}$~$3.4\text{x}10^{38}$
230	$1725436586697640946858688965569256363112777243042596638790631055949824=2^{230}$~$10^{100}$

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

One serious problem for public-key cryptography

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor

AT&T Bell Labs

In Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20-22, 1994, IEEE Computer Society Press, pp. 124-134.

Also a nuisance for symmetric key cryptography

A fast quantum mechanical algorithm for database search

Lov K. Grover

AT&T Bell Labs

In Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pp. 212-219

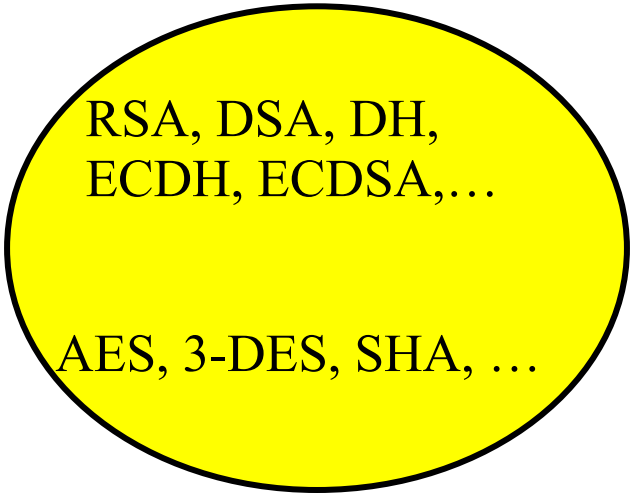
How secure will our current crypto algorithms be?

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?

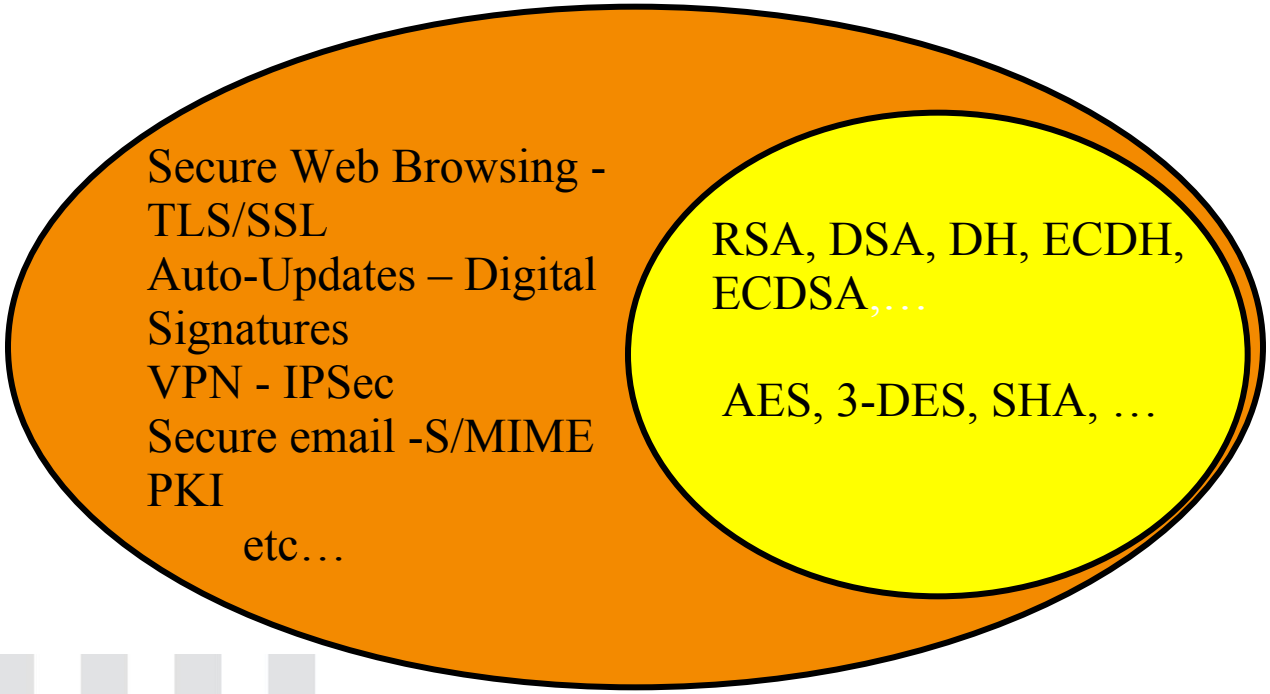
Public-key cryptosystems based on factoring and discrete logarithms (including elliptic curve discrete logarithms) are broken by efficient attacks.

Symmetric-key systems are weakened by stronger brute-force attacks.



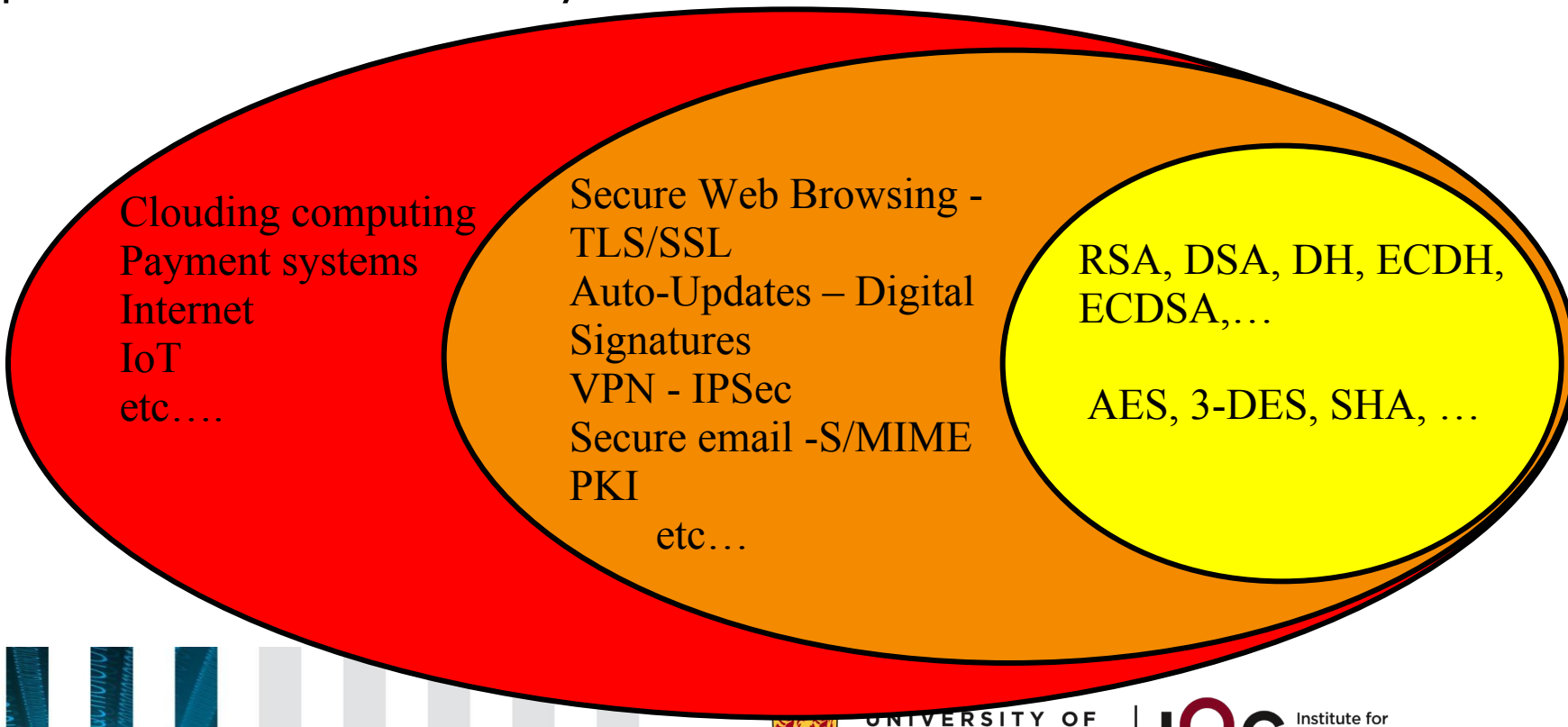
What will be affected?

Breaking or weakening this fundamental cryptography protocols will undermine the security protocols that rely on them.



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.

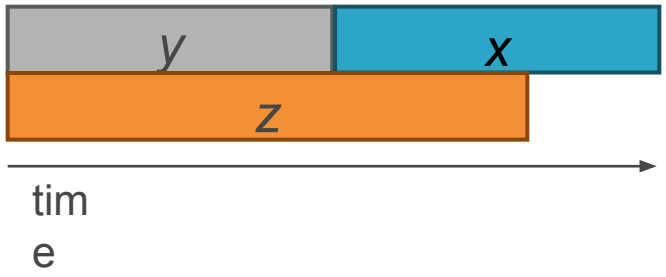


How much of a problem is quantum computing, really?

How soon do we need to worry?

Depends on*:

- How long do you need your cryptographic keys to be secure? – *security shelf-life* (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years) – *migration time*
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (*z* years) – *collapse time*
- "Theorem": If $x + y > z$, then worry.



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

Business 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.

- **Prediction:** In the next 6-24 months, organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan.

Managing the quantum risk

•At a high level, we need to assess x,y and z for the range of information assets and business functions.

→ Urgent action required to minimize losses

Security Shelf life | **Migration Time** | **Collapse Time**

→ Acting now will avoid losses

Quantum-safe cryptographic tool-chest

quantum-resistant conventional 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 secure against quantum attacks

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

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

How easy is it to evolve from one cryptographic algorithm to a quantum-secure one?

Are the standards and practices ready?

Building a large quantum computer

REVIEW

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret[1,2] and R. J. Schoelkopf[1]*

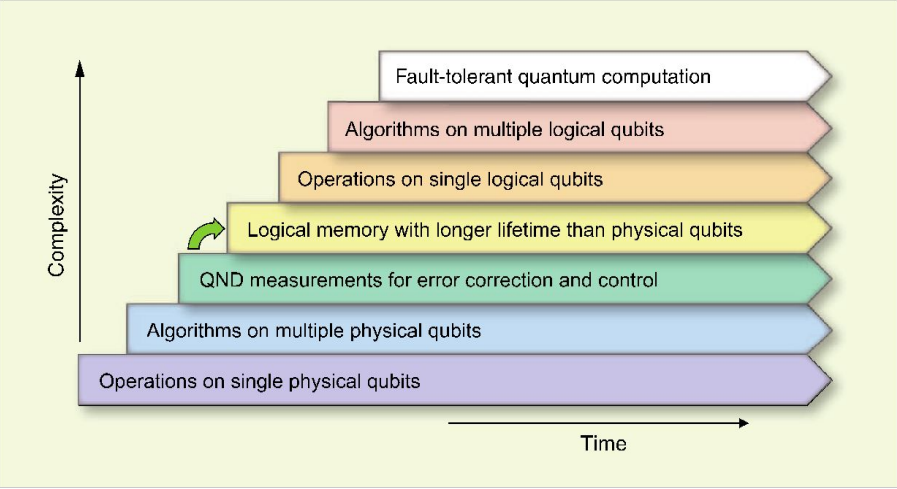


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

SCIENCE VOL 339 8 MARCH 2013

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Building a large quantum computer

- "Stage 4" is a critical step of building a quantum computer capable of implementing the algorithms that are known to threaten cryptography.
- Great progress continues to be made toward the design of a scalable fault-tolerant quantum computer.
- Continued investment, e.g.:
  - 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."*
  - IBM [December 2015] *"IBM Awarded IARPA Grant to Advance Research Towards a Universal Quantum Computer; IBM scientists will focus on building the first logical quantum bit"*

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.*

NSA [August 2015]: *NSA's Information Assurance Directorate "will initiate a transition to quantum resistant algorithms in the not too distant future."* https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

NSA [January 2016]: *CNSA Suite and Quantum Computing FAQ* https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm

NIST [February 2016]: *NISTIR 8105 DRAFT Report on Post-Quantum Cryptography "outlines NIST's initial plan to move forward in this space".*
http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf

ETSI white paper: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

What do we do today?

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.
michele.mosca@evolutionq.com

•Upcoming workshop of interest:
4th ETSI/IQC Workshop on Quantum-Safe Cryptography
19-21 September 2016
Toronto, Canada