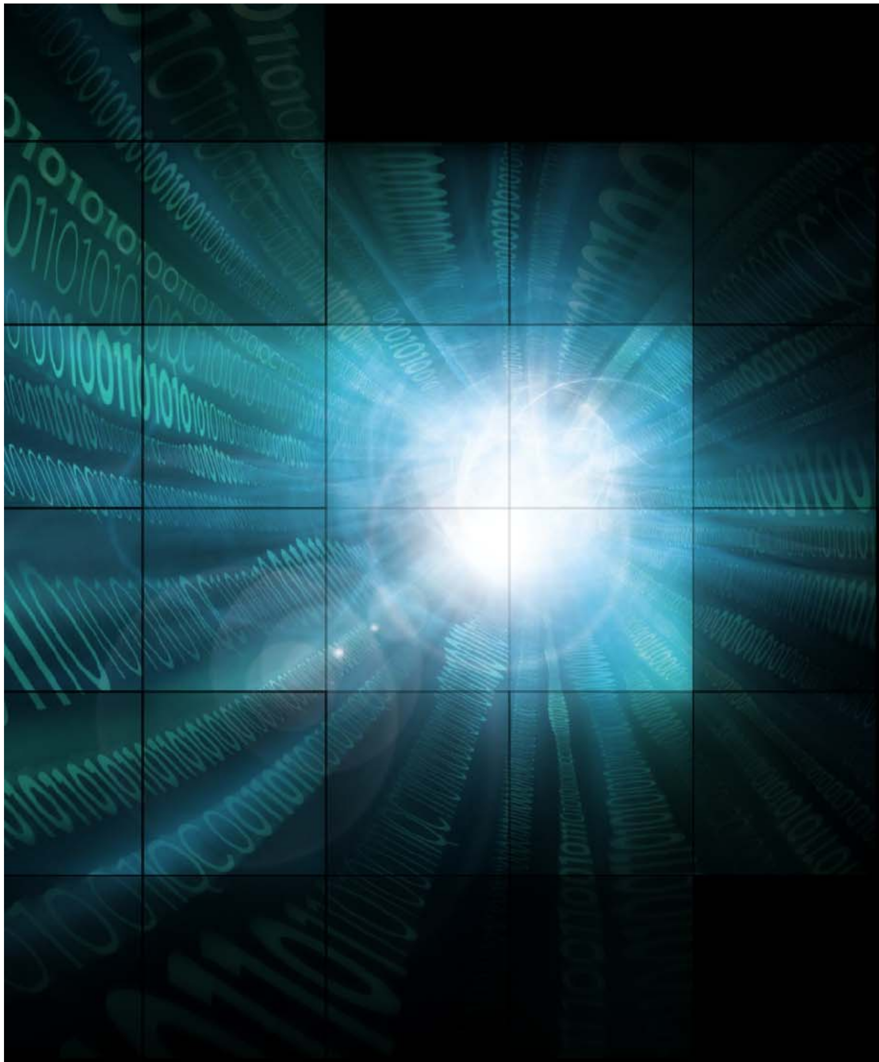
AWACS 2016



The quantum threat to cryptography

Michele Mosca
8 May 2016

Vienna, Austria

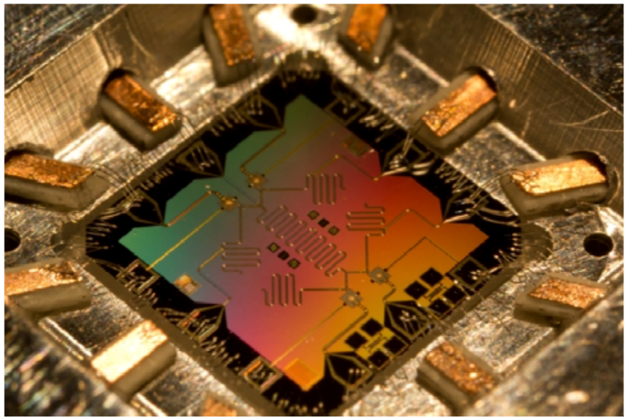
PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

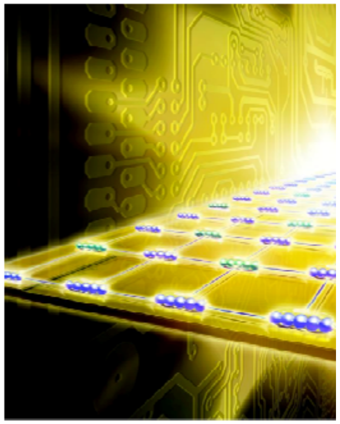
evolutionQ

CryptoWorks21

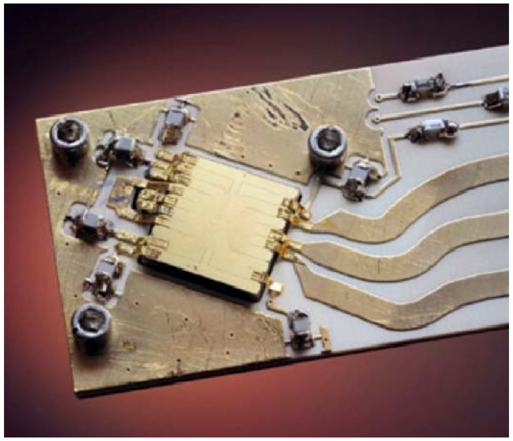
Cryptography in the context of quantum computers



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



© Harald Ritsch



Y. Colombe/NIST

evolutionQ

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

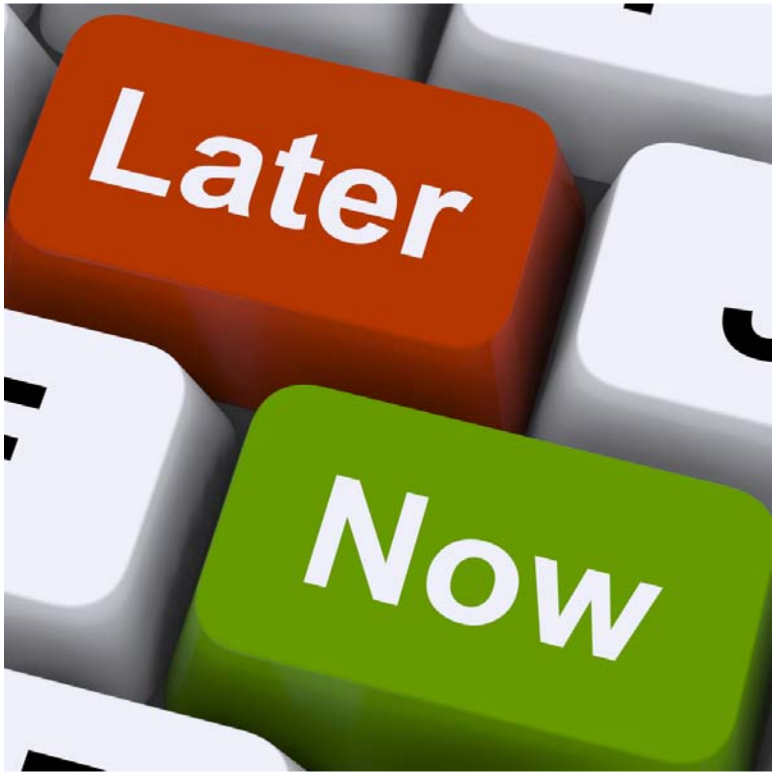
How secure will our current crypto algorithms be?

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

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

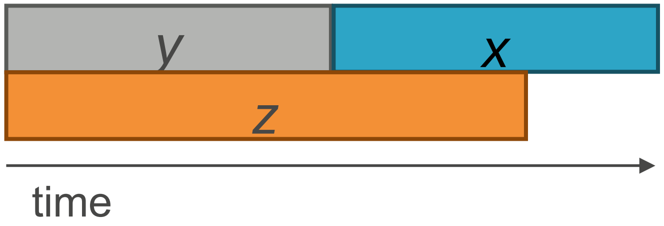
How much of a problem is quantum computing, really?



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.

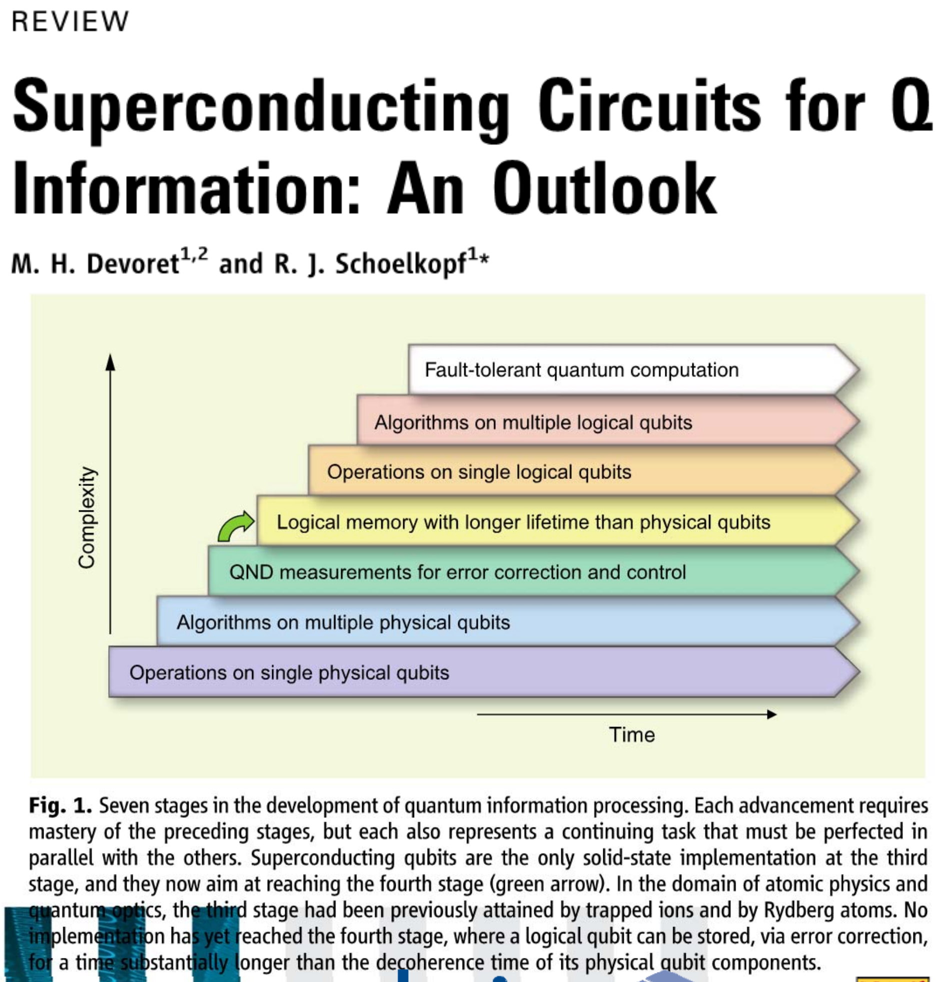
NSA [August 2015]: *NSA's Information Assurance Directorate "will initiate a transition to quantum resistant algorithms in the not too distant future."*
https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

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 [April 2016]: *NISTIR 8105 Report on Post-Quantum Cryptography "outlines NIST's initial plan to move forward in this space".*
http://dx.doi.org/10.6028/NIST.IR.8105

ETSI white paper [2014]:
http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

Building a large quantum computer



REVIEW

Superconducting Circuits for Quantum Information: An Outlook

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

Fault-tolerant quantum computation
Algorithms on multiple logical qubits
Operations on single logical qubits
Logical memory with longer lifetime than physical qubits
QND measurements for error correction and control
Algorithms on multiple physical qubits
Operations on single physical qubits
Complexity
Time

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

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.

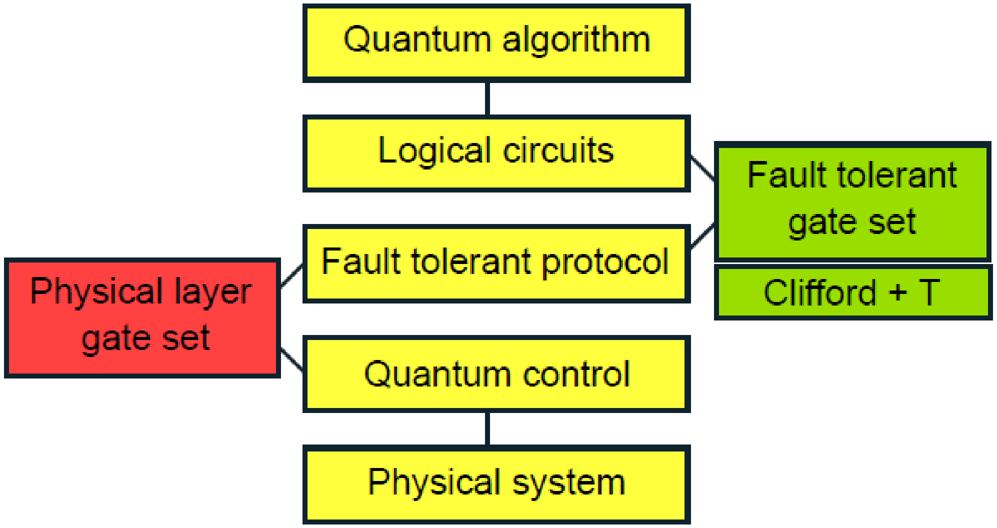
What I don't worry about

- Implementations of quantum factoring to date (except where they demonstrate meaningful benchmarks towards fault-tolerance)

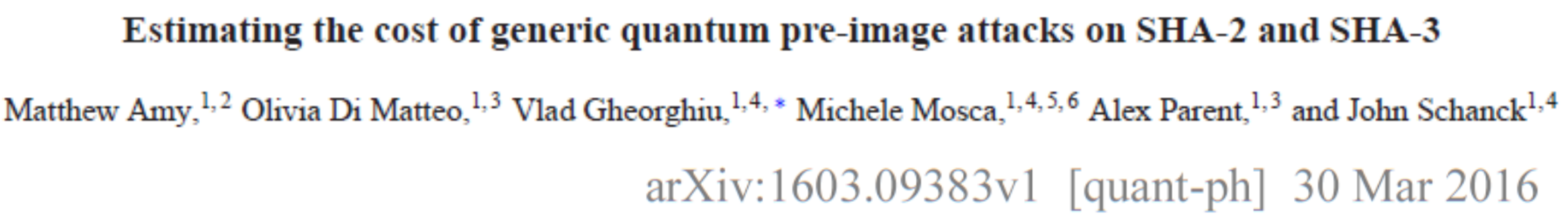
- "Quantum computing" approaches that do not have an articulated plan for fault-tolerantly implementing quantum algorithms such as Shor's and Grover's.

Quantum compilers

The efficiency of each step in the translation from high level algorithm to physical device impacts the efficiency of quantum attacks.



Quantum cost estimation

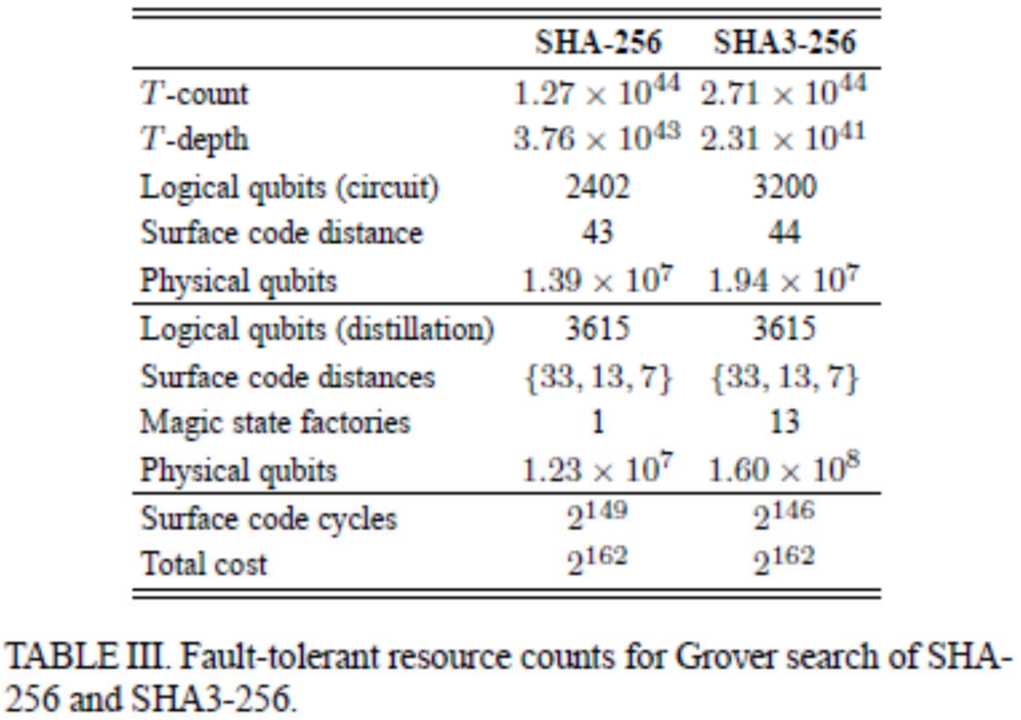


Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3

Matthew Amy,[1,2] Olivia Di Matteo,[1,3] Vlad Gheorghiu,[1,4,*] Michele Mosca,[1,4,5,6] Alex Parent,[1,3] and John Schanck[1,4]

arXiv:1603.09383v1 [quant-ph] 30 Mar 2016

The efficiency of each step in the translation from high level algorithm to physical device impacts the efficiency of quantum attacks.



	SHA-256	SHA3-256
T-count	1.27×10^{44}	2.71×10^{44}
T-depth	3.76×10^{43}	2.31×10^{41}
Logical qubits (circuit)	2402	3200
Surface code distance	43	44
Physical qubits	1.39×10^{7}	1.94×10^{7}
Logical qubits (distillation)	3615	3615
Surface code distances	$\{33, 13, 7\}$	$\{33, 13, 7\}$
Magic state factories	1	13
Physical qubits	1.23×10^{7}	1.60×10^{8}
Surface code cycles	2^{149}	2^{146}
Total cost	2^{162}	2^{162}

TABLE III. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

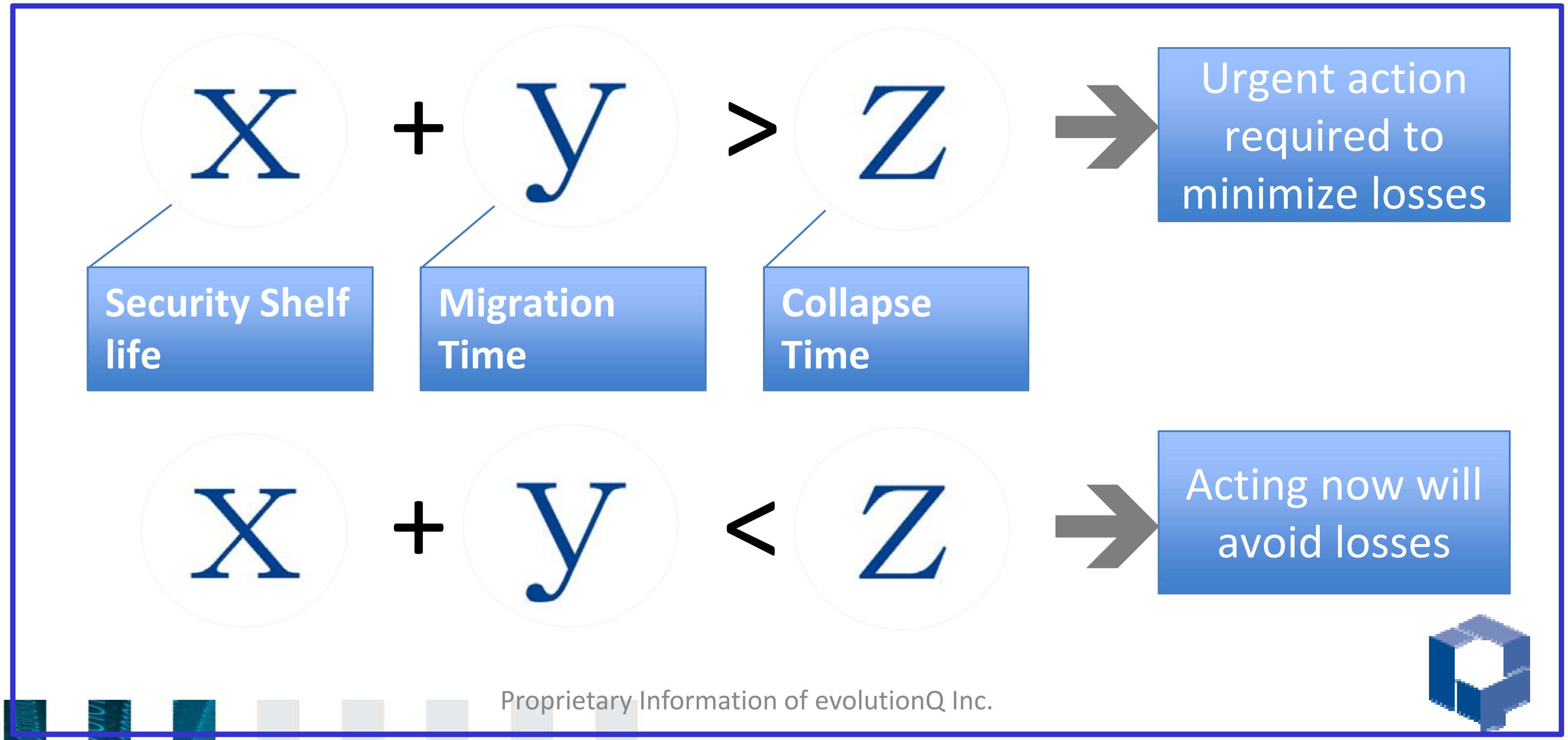
What is ‘z’?

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.*

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.



$x + y > z$ → Urgent action required to minimize losses

x: Security Shelf life

y: Migration Time

z: Collapse Time

$x + y < z$ → Acting now will avoid losses

Assessing and managing ‘y’

- This is the part of the equation we have some control over.

- We have known about this threat since 1994.
- Progress on building large-scale quantum computers has been public and relatively gradual.
- So there is no fundamental reason for panic or rush.
- To avoid a future panic or rush, we need a concerted effort now.

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

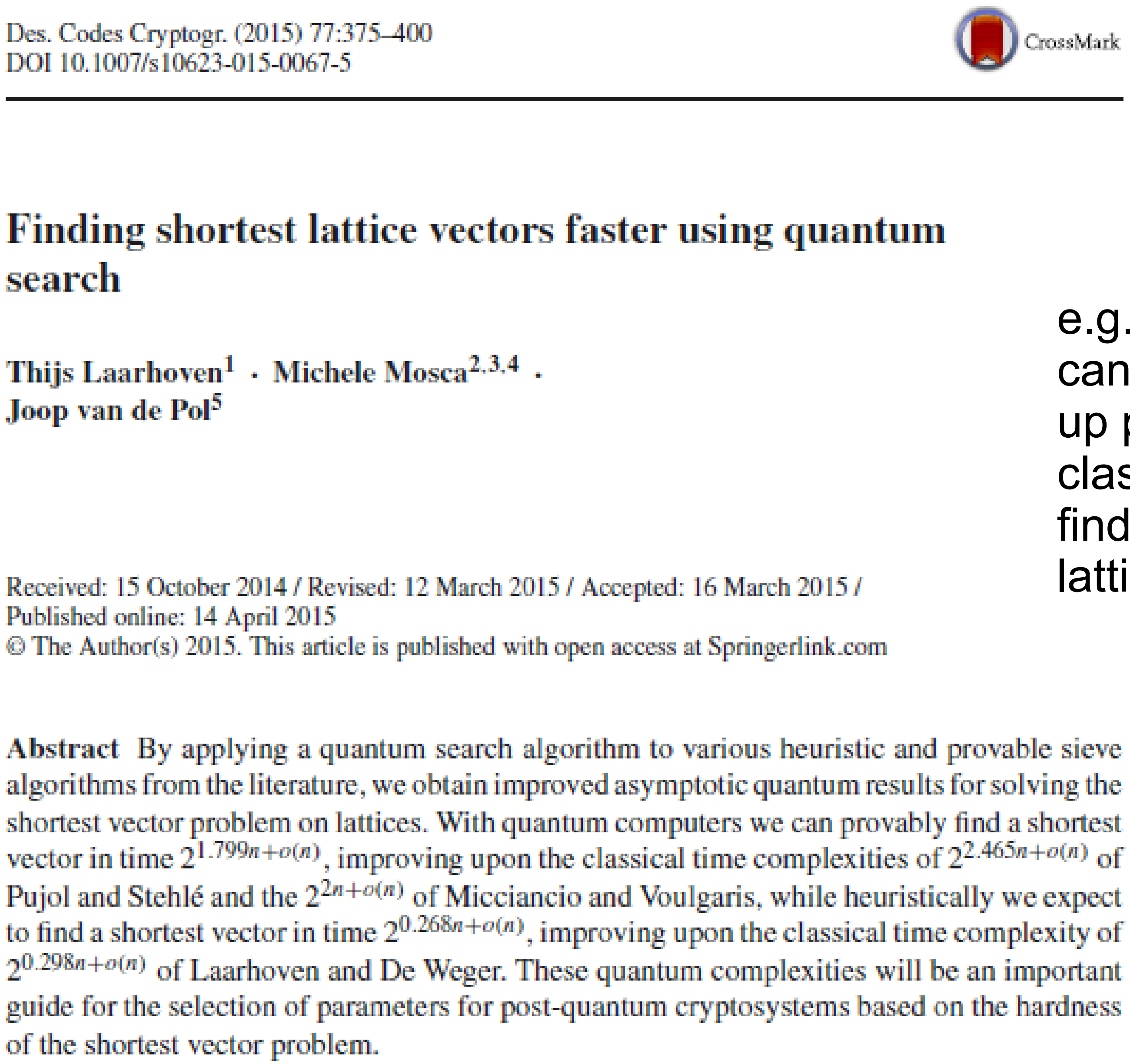
Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem

Is Quantum Key Establishment (QKD) “out-of-band”? i.e. comparable to trusted courier?

Protocol	Uses untrusted communication channel?	Uses any standard telecommunications channels?
Post-quantum	YES	YES
Trusted Courier	NO	NO
QKD	YES	NO

Are we ready to deploy post-quantum crypto?

- Promising approaches include hash-based signatures, lattice-based, code-based, multi-variate equation based, elliptic curve isogenies, …
- In various stages of readiness. Some are quite mature. Still require further work on robust implementation and integration into applications.
- **But quantum algorithmic analysis has been quite limited.** Much more work is needed to achieve high levels of confidence. One mitigation strategy is to use post-quantum in a "hybrid" fashion with ECC.



Des. Codes Cryptogr. (2015) 77:375–400
DOI 10.1007/s10623-015-0067-5

Finding shortest lattice vectors faster using quantum search

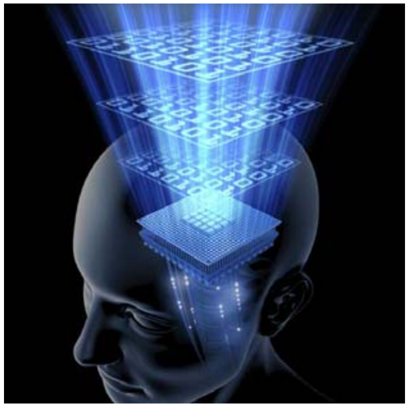
Thijs Laarhoven[1] · Michele Mosca[2,3,4] ·
Joop van de Pol[5]

Received: 15 October 2014 / Revised: 12 March 2015 / Accepted: 16 March 2015 /
Published online: 14 April 2015

Abstract By applying a quantum search algorithm to various heuristic and provable sieve algorithms from the literature, we obtain improved asymptotic quantum results for solving the shortest vector problem on lattices. With quantum computers we can provably find a shortest vector in time $2^{1.799n+o(n)}$, improving upon the classical time complexities of $2^{2.465n+o(n)}$ of Pujol and Stehlé and the $2^{2n+o(n)}$ of Micciancio and Voulgaris, while heuristically we expect to find a shortest vector in time $2^{0.268n+o(n)}$, improving upon the classical time complexity of $2^{0.298n+o(n)}$ of Laarhoven and De Weger. These quantum complexities will be an important guide for the selection of parameters for post-quantum cryptosystems based on the hardness of the shortest vector problem.

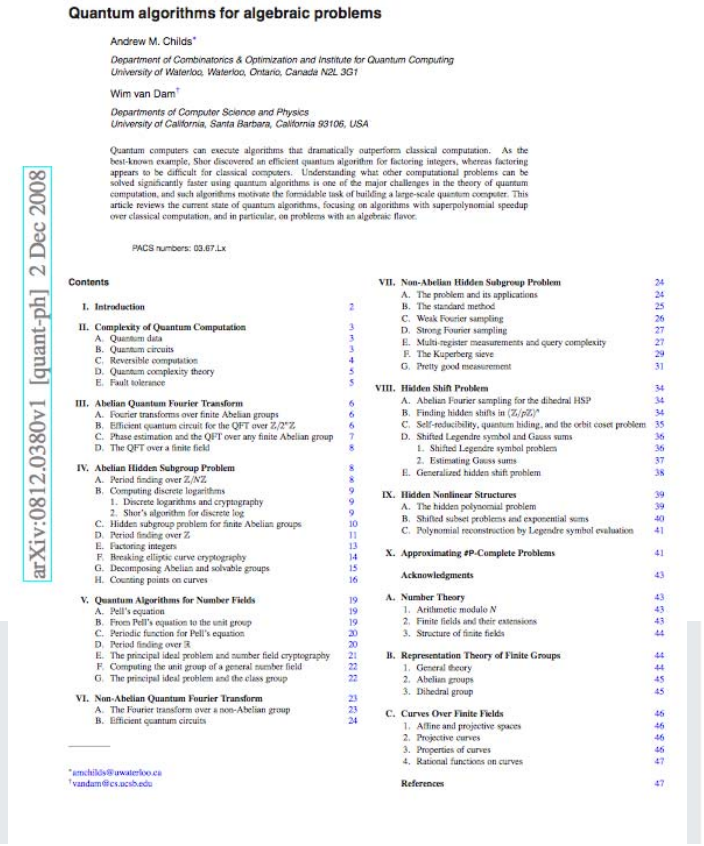
e.g. quantum searching can be applied to speed up parts of complex classical algorithms, e.g. finding short vectors in a lattice.

NEW ALGORITHMS AND ALGORITHIC PARADIGMS



UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

http://math.nist.gov/quantum/zoo/ *(maintained by S. Jordan)*



arXiv:0812.0380v1 [quant-ph] 2 Dec 2008

Quantum algorithms for algebraic problems

Andrew M. Childs[*]

Department of Combinatorics & Optimization and Institute for Quantum Computing
University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Wim van Dam[†]

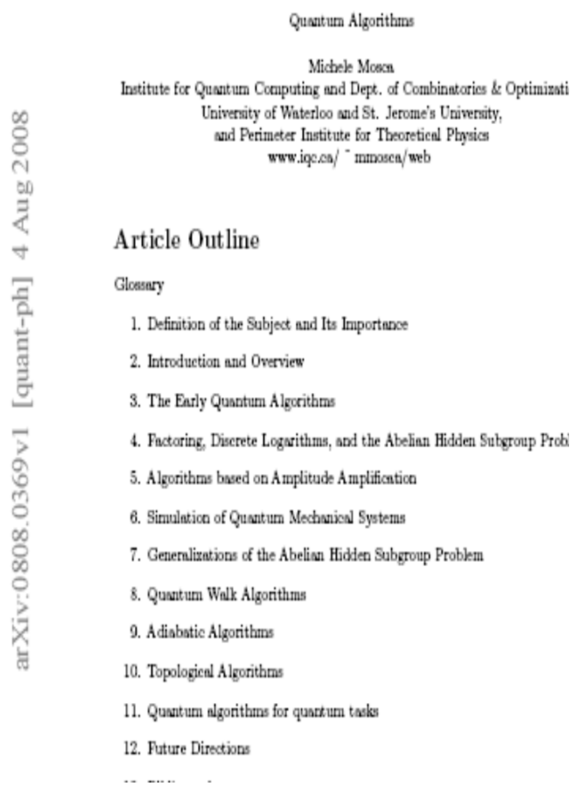
Departments of Computer Science and Physics
University of California, Santa Barbara, California 93106, USA

Quantum computers can execute algorithms that dramatically outperform classical computation. As the best-known example, Shor discovered an efficient quantum algorithm for factoring integers, whereas factoring appears to be difficult for classical computers. Understanding what other computational problems can be solved significantly faster using quantum algorithms is one of the major challenges in the theory of quantum computation, and such algorithms motivate the formidable task of building a large-scale quantum computer. This article reviews the current state of quantum algorithms, focusing on algorithms with superpolynomial speedup over classical computation, and in particular, on problems with an algebraic flavor.

PACS numbers: 03.67.Lx

Contents

[*] amchilds@uwaterloo.ca
[†] vandam@cs.ucsb.edu



arXiv:0808.0369v1 [quant-ph] 4 Aug 2008

Quantum Algorithms

Michele Mosca
Institute for Quantum Computing and Dept. of Combinatorics & Optimizati
University of Waterloo and St. Jerome's University,
and Perimeter Institute for Theoretical Physics
www.iqc.ca/ ˜ mmosca/web

Article Outline

arXiv:1001.0767v2 [quant-ph] 7 Jan 2010

Algorithms for Quantum Computers

Jamie Smith and Michele Mosca

1 Introduction

Quantum computing is a new computational paradigm created by reformulating information and computation in a quantum mechanical framework [30, 27]. Since the laws of physics appear to be quantum mechanical, this is the most relevant framework to consider when considering the fundamental limitations of information processing. Furthermore, in recent decades we have seen a major shift from just observing quantum phenomena to actually controlling quantum mechanical systems. We have seen the communication of quantum information over long distances, the "teleportation" of quantum information, and the encoding and manipulation of quantum information in many different physical media. We still appear to be a long way from the implementation of a large-scale quantum computer, however it is a serious goal of many of the world's leading physicists, and progress continues at a fast pace.

In parallel with the broad and aggressive program to control quantum mechanical systems with increased precision, and to control and interact a larger number of subsystems, researchers have also been aggressively pushing the boundaries of what useful tasks one could perform with quantum mechanical devices. These in-

Jamie Smith
Institute for Quantum Computing and Dept. of Combinatorics & Optimization
University of Waterloo,
with support from the Natural Sciences and Engineering Research Council of Canada
e-mail: ja5smith@iqc.ca

Michele Mosca
Institute for Quantum Computing and Dept. of Combinatorics & Optimization
University of Waterloo and St. Jerome's University,
and Perimeter Institute for Theoretical Physics,
with support from the Government of Canada, Ontario-MRI, NSERC, QuantumWorks, MITACS, CIFAR, CRC, ORF, and DTO-ARO
e-mail: mmosca@iqc.ca

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

Are the standards and practices ready?

Standards activities:

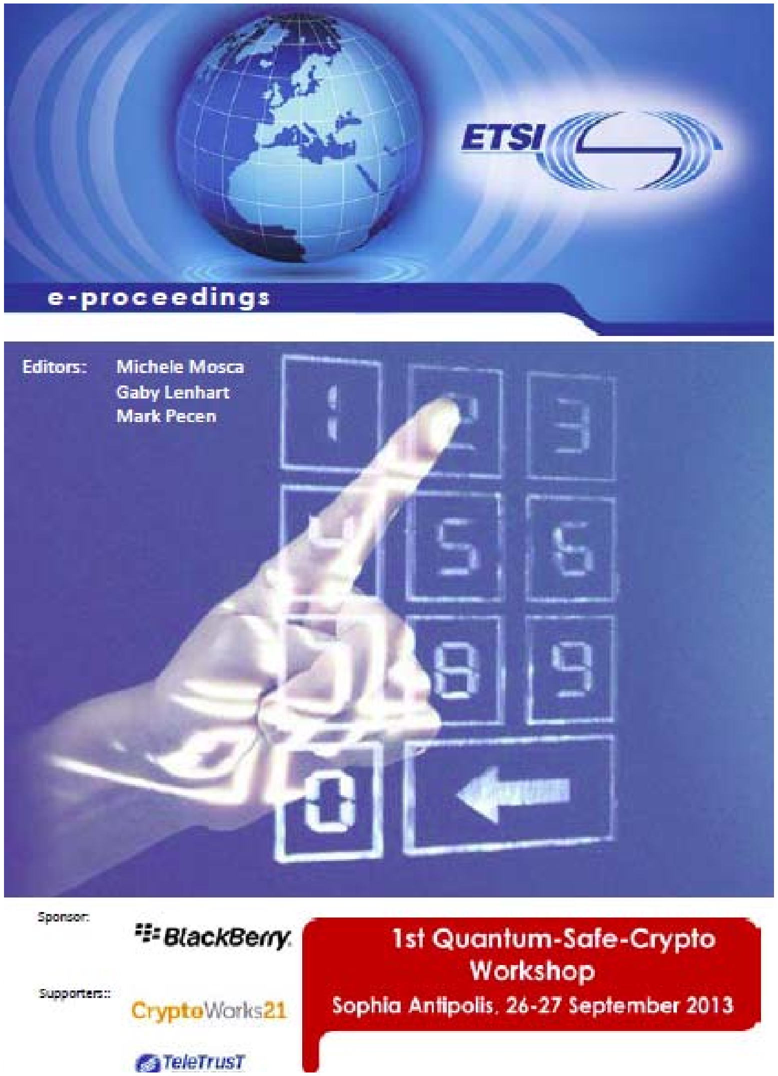
ETSI ISG on Quantum Key Distribution (since 2008)

Scope:

To develop GSs (ETSI Group Specifications) describing quantum cryptography for ICT networks. Quantum Key Distribution is the essential credential in order to use quantum cryptography on a broad basis. It is the main task of the QKD ISG to specify a system for Quantum Key Distribution and its environment.

The activities of the QKD ISG will be performed in close co-operation with relevant standards activities within and outside ETSI. External relationships will be established where and when ever needed, Formal relationships will be established using the normal ETSI processes via the ETSI Secretariat.

Standards activities:



ETSI

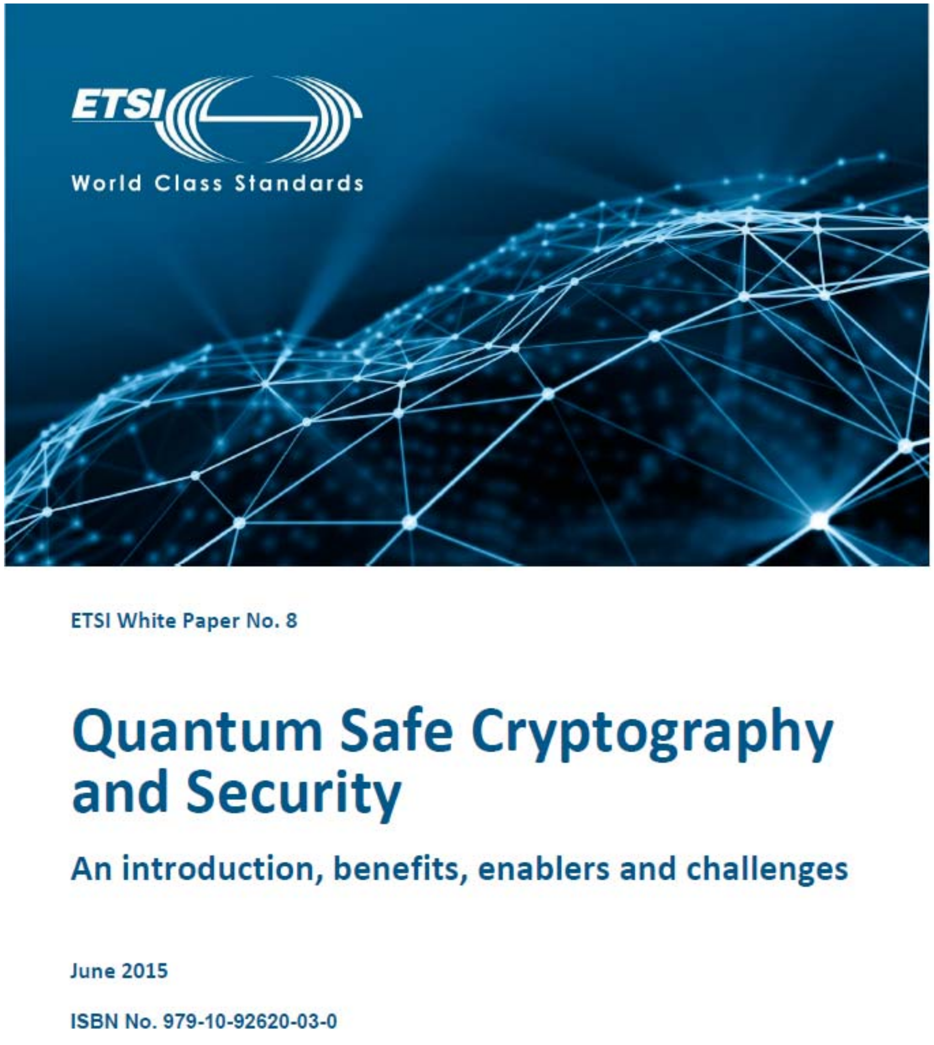
e-proceedings

Editors: Michele Mosca
Gaby Lenhart
Mark Pecen

Sponsor: BlackBerry

Supporters:: CryptoWorks21
TeleTrusT

1st Quantum-Safe-Crypto Workshop
Sophia Antipolis, 26-27 September 2013



ETSI
World Class Standards

ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges

June 2015

ISBN No. 979-10-92620-03-0

Standards activities:

ETSI 2nd Quantum-Safe Crypto Workshop in partnership with the IQC
6 - 7 October, 2014, Ottawa, Canada

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography, hosted by SK Telecom
5-7 October, 2015, Seoul, Korea

4th ETSI/IQC Workshop on Quantum-Safe Cryptography
19-21 September, 2016, Toronto, Canada

Standards activities:

ETSI ISG on Quantum Safe Cryptography (since 2015)

- Focus is on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, benchmarking and practical architectural considerations
- Currently hold 5 regular meetings each year at ETSI headquarters in Sophia Antipolis, France
- The work may feed into other standards groups.

IETF

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

ISO

International Organization for Standardization

NICT

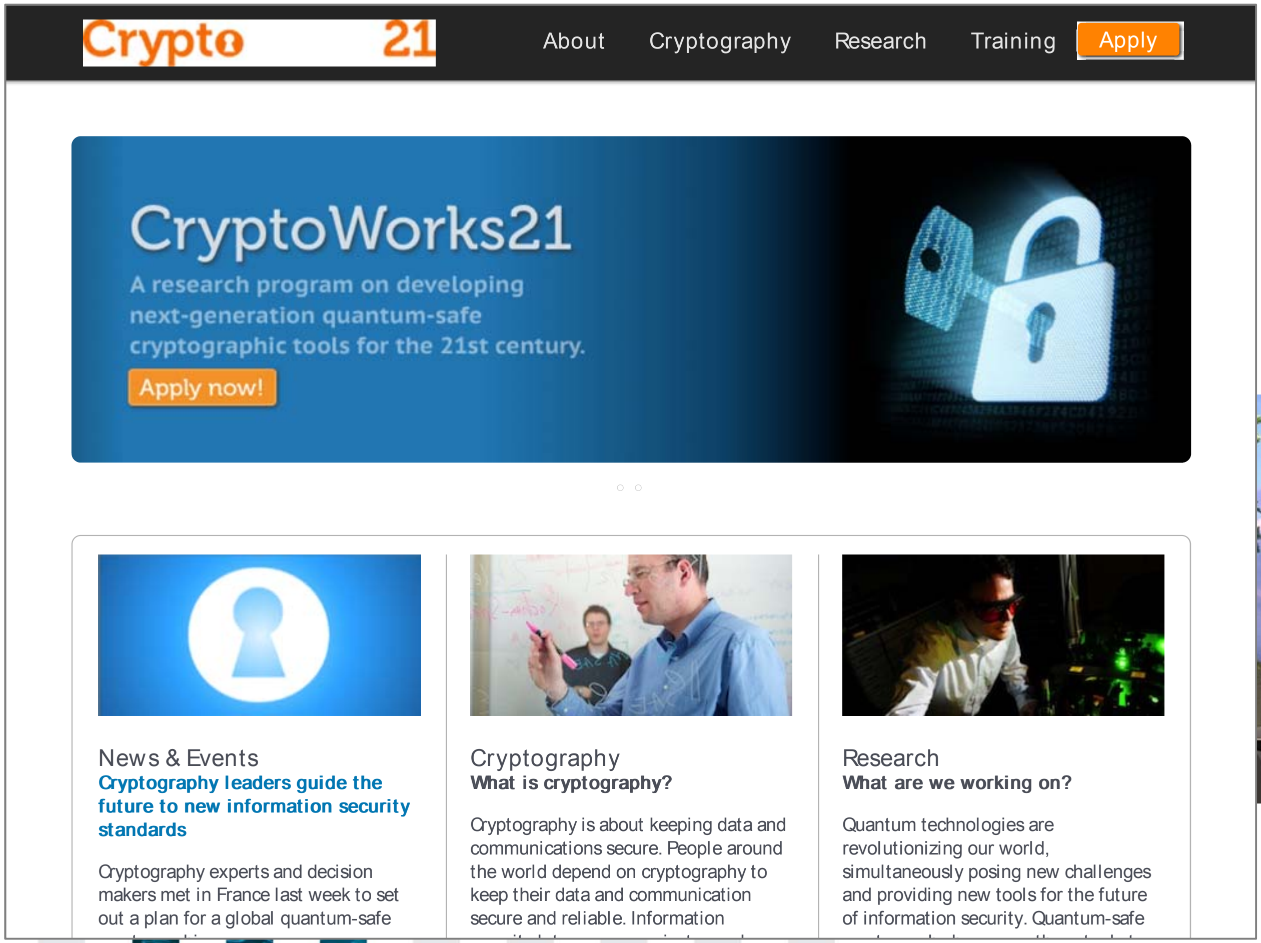
National Institute of Information and Communications Technology

evolutionQ

UNIVERSITY OF WATERLOO

IQC Institute for Quantum Computing

Preparing the workforce: *cryptoworks21.com*



CryptoWorks21

A research program on developing next-generation quantum-safe cryptographic tools for the 21st century.

News & Events

Cryptography leaders guide the future to new information security standards

Cryptography experts and decision makers met in France last week to set out a plan for a global quantum-safe

Cryptography

What is cryptography?

Cryptography is about keeping data and communications secure. People around the world depend on cryptography to keep their data and communication secure and reliable. Information

Research

What are we working on?

Quantum technologies are revolutionizing our world, simultaneously posing new challenges and providing new tools for the future of information security. Quantum-safe

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

What do we do today?

evolutionQ

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Suggestions

- Get quantum-safe options on roadmaps
  - Routinely ask about vulnerability of systems to quantum attacks
  - Include quantum-safe options as desired features
  - Keep switching costs low
- Make quantum risk management a part of cybersecurity roadmaps
- (If appropriate) request the standards for the quantum-safe tools needed
- Request the information/studies needed to make wise decisions going forward.
- Encourage (quantum and classical) cryptanalysis of post-quantum schemes, and benchmarking of post-quantum tools.
- Applaud and reward organizations that take this seriously.

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