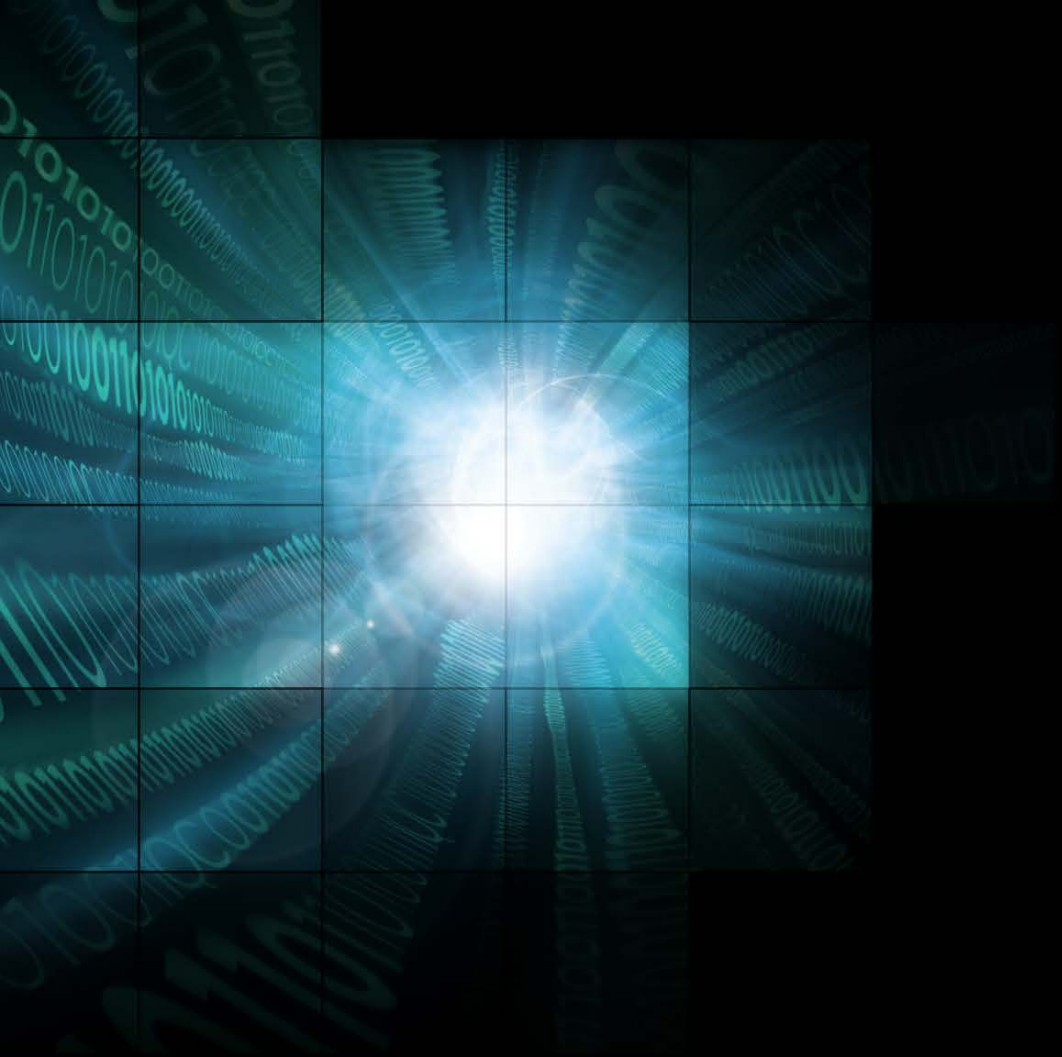


Cybersecurity in a Quantum World: will we be ready?

Michele Mosca

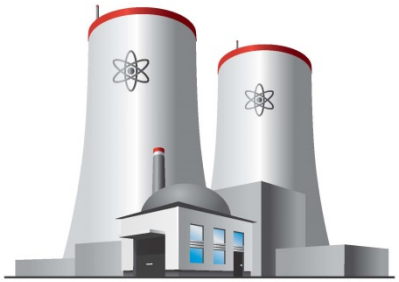
University Research Chair

3 April 2015

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

CryptoWorks21



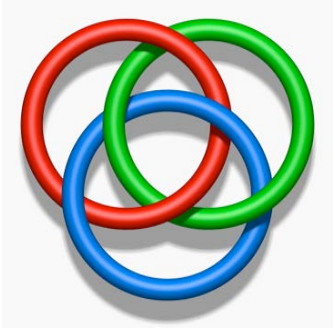
NUCLEAR POWER STATION

Cyber technologies are becoming increasingly pervasive.

Cybersecurity is a growing and fundamental part of safety and security of individuals, organizations and society.

Cryptography is a foundational pillar of cybersecurity

Cryptography allows us to achieve information security while using untrusted communication systems.

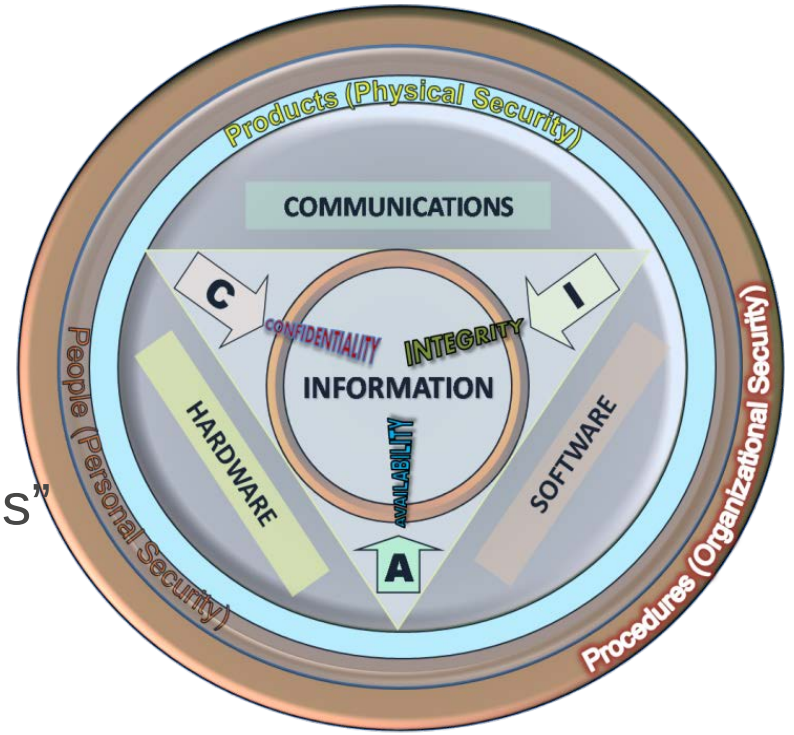


e.g. Do you update your software and anti-virus daily? Why do you trust the source?

A foundational pillar for a complex system

Many potential weak links:

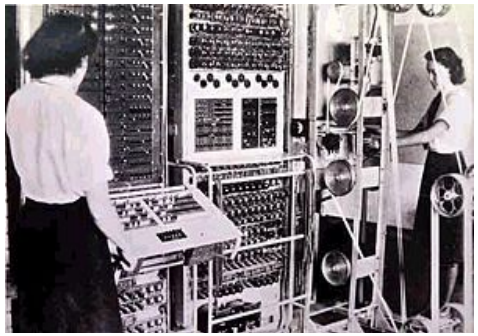
- bad trust assumptions
- phishing
- weak passwords
- bad implementations
- side-channel attacks
- cryptography protocol errors
- etc, etc.
- … including … “unknown unknowns”



Most cryptographic algorithms are based on a computational assumption.

One family of codes (before the era of “modern cryptography”) that were believed to be computationally secure were the “Fish” codes used in WWII.

commons.wikimedia.org/wiki/Image:Colossus.jpg



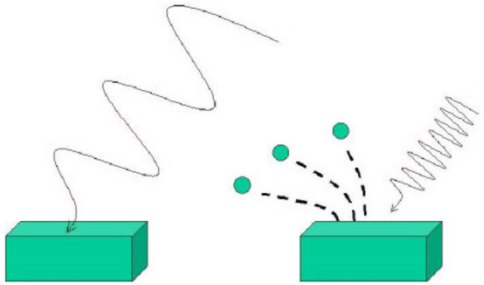
Prof. Bill Tutte was responsible for cracking these codes (see http://math.uwaterloo.ca/combinatorics-and-optimization/about/professor-william-t-tutte for more information). In 1943, the electronic computer COLOSSUS was designed and built by the British Post Office in order to run the algorithms that Tutte and collaborators developed.

The “Waterloo algorithm” for the “discrete logarithm” problem (I. F. Blake, R. Fuji-Hara, R. C. Mullin and S. A. Vanstone, 1984) broke a discrete logarithm based scheme. This showed that the scheme implemented by MITRE (in software) and then on a prototype chip by Hewlett-Packard.

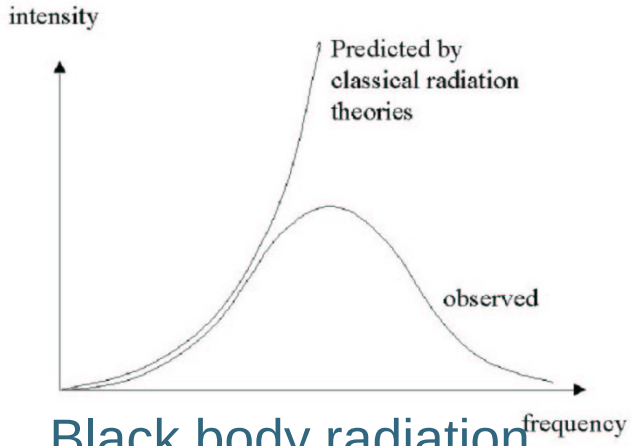


A NEW PARADIGM FOR PHYSICS

Signatures of quantum mechanics

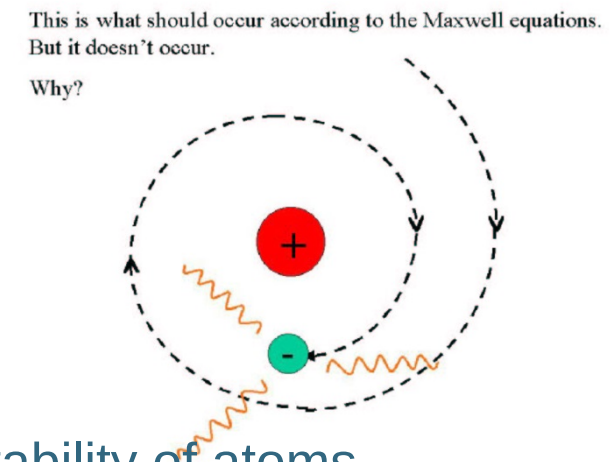


Photoelectric effect



Black body radiation

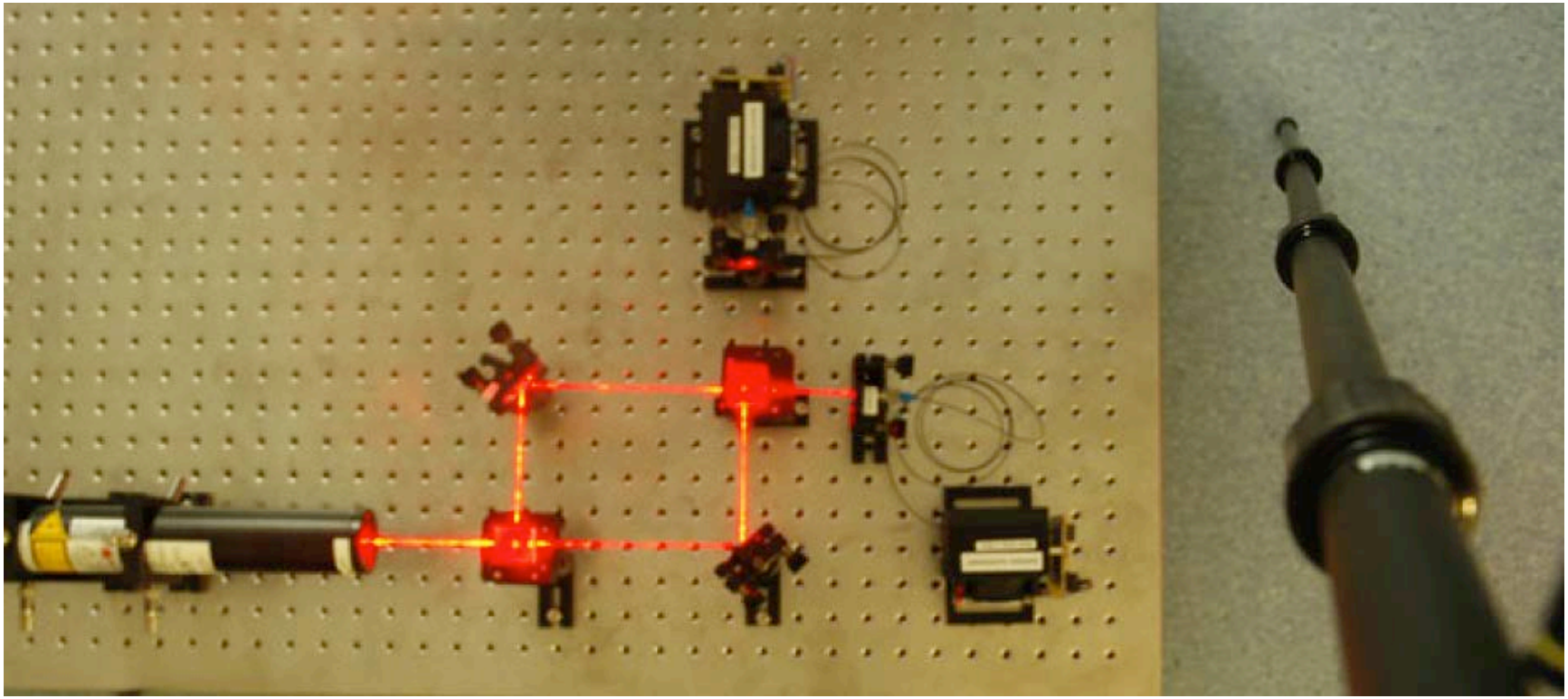
Atomic radiation spectrum



Stability of atoms

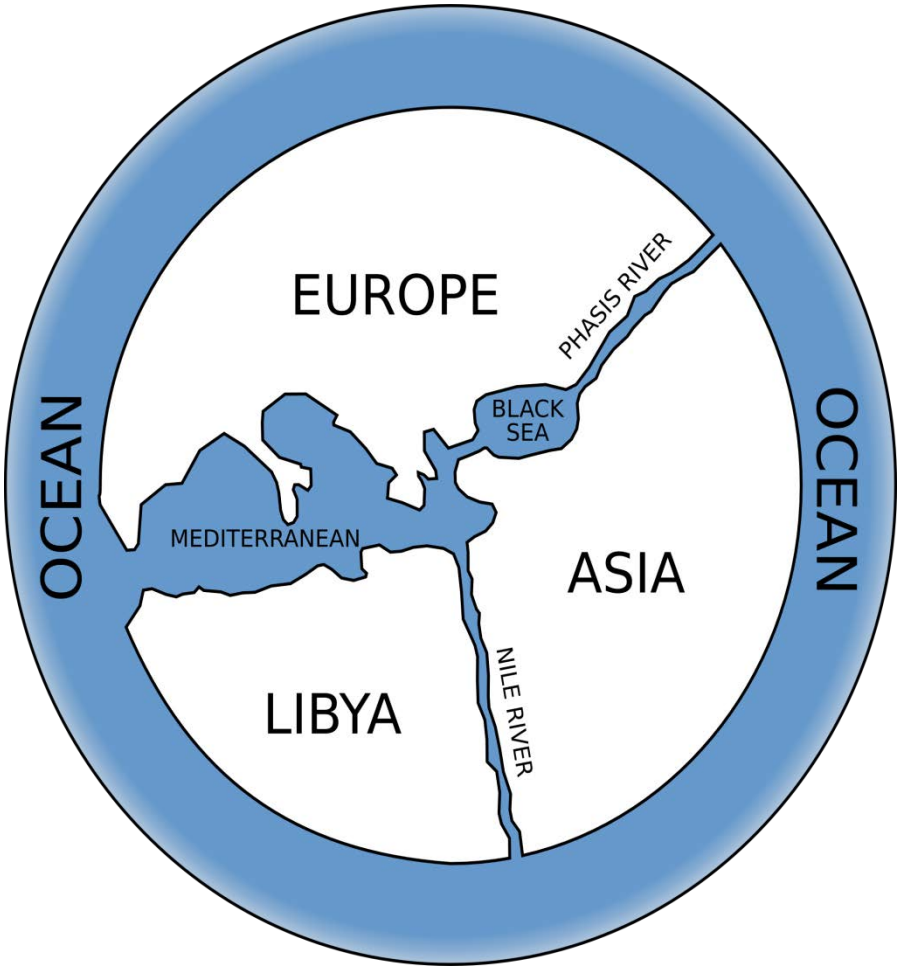
CryptoWorks21

Quantum Interference

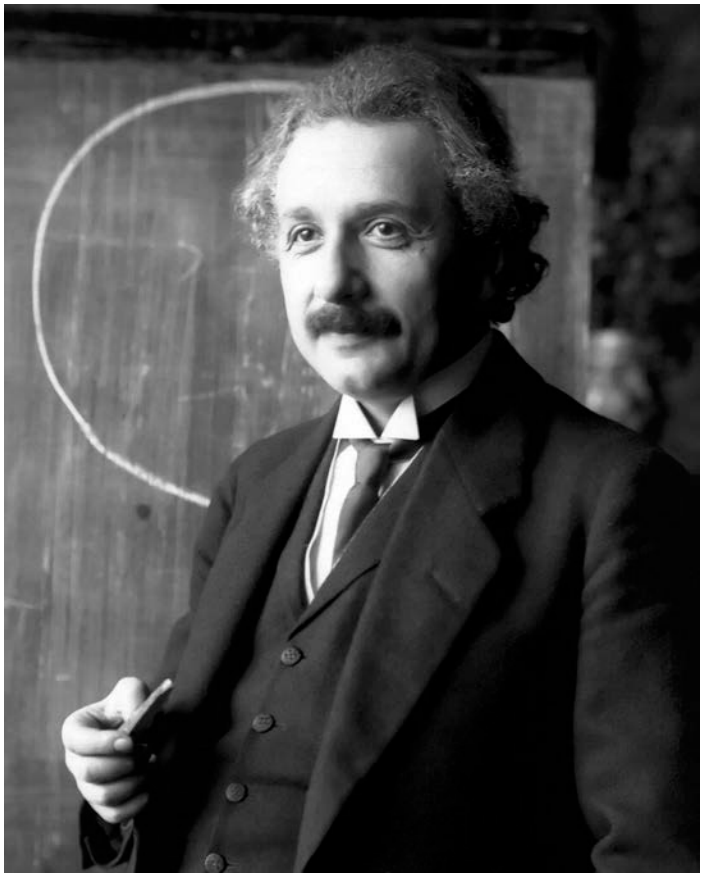


- Dave Bacon's photo of Antia Lamas-Linares' lab at NUS Singapore

A new mathematical paradigm



…a new paradigm…



The new paradigm was not immediately accepted…even by some of its founders.

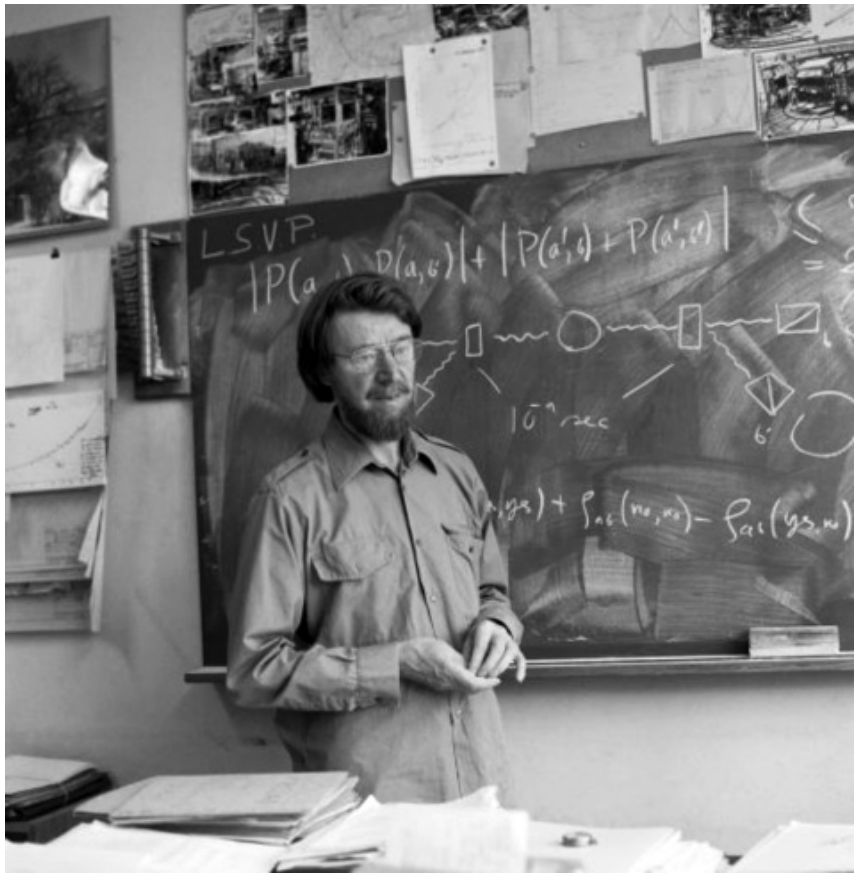
- “The more success the quantum theory has, the sillier it looks.”
  - To Heinrich Zangger, 1912
- "I believe, however, that [quantum] theory offers no useful point of departure for future development.”
  - Autobiographical notes, 1951.

…a new paradigm…

Max Planck:

- “A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it.”

- The new paradigm for physics had implications that many people were uncomfortable with.
- John Bell proposed an experimental test that would distinguish a large class of classical theories people were hoping could be used instead of quantum theory.



- In the early 1980s Alain Aspect provided the first experimental verification of the “Bell Inequalities”, verifying quantum theory and contradicting classical “local hidden variable theories”.

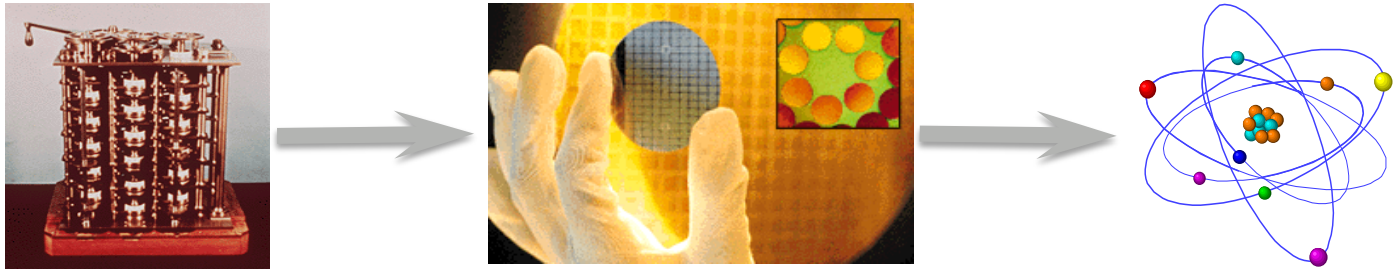
…a new paradigm…

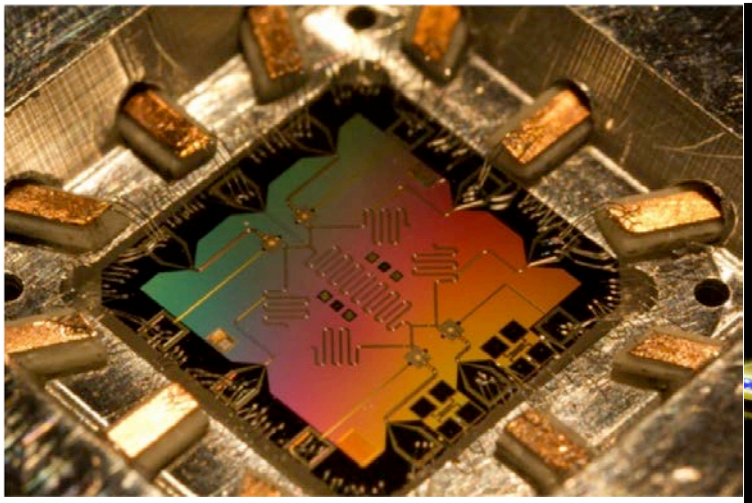
- The quantum paradigm eventually became the dominant paradigm for physics.

- This new paradigm for physics eventually challenged the traditional paradigm for computation…

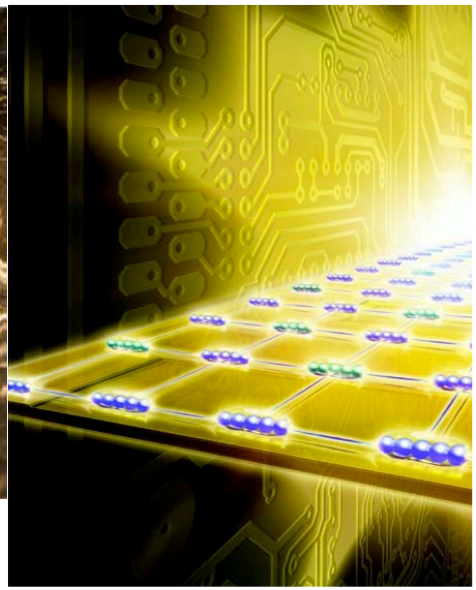
Physics and Computation

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

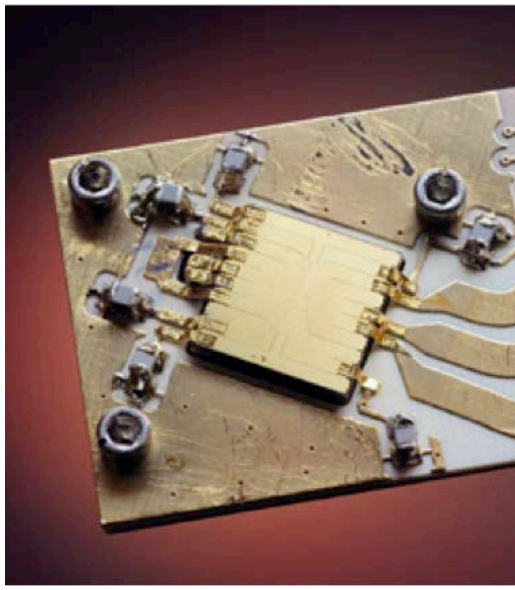




E. Lucero, D. Mariantoni, and M. Mariantoni

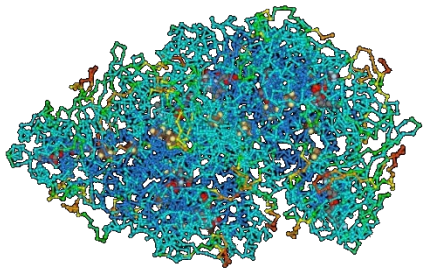


© Harald Ritsch

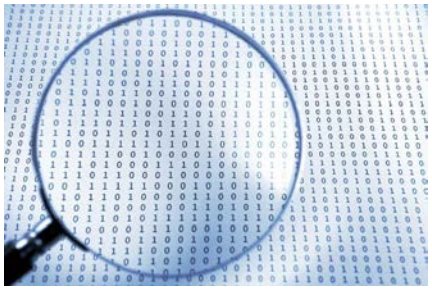


Y. Colombe/NIST

The quantum paradigm leads us to a host of new technologies that can solve important problems in computation, communication and sensing.



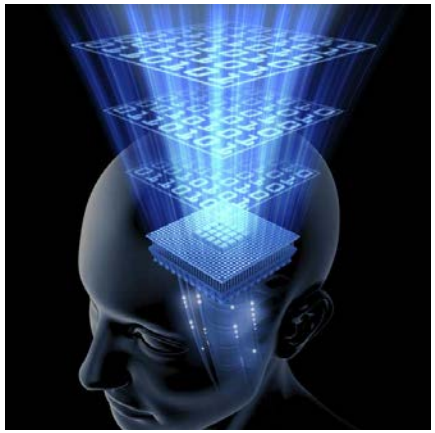
Simulating quantum mechanical systems



General searching, counting, and optimizing

Better sensing and metrology

Image: CC-BY-SA 2005 Nachoman-au en.wikipedia.org/wiki/Image:Magellan_GPS_Blazer12.jpg



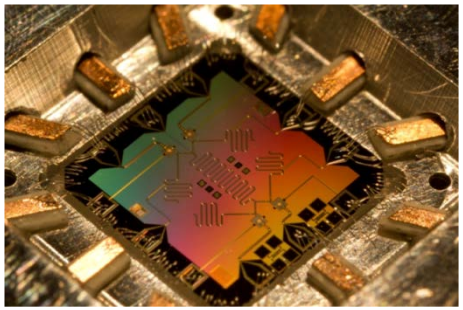
Future discoveries…

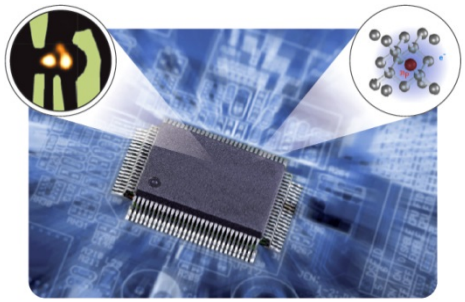
One serious problem for public-key cryptography

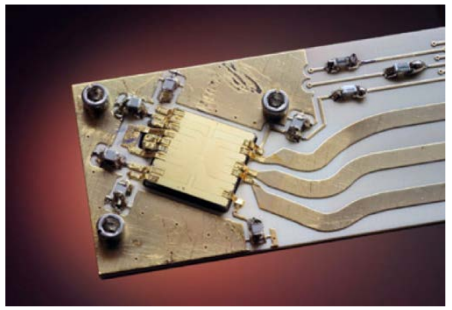
In: Proceedings, 35th Annual Symposium on Foundations of Computer Science,
Santa Fe, NM, November 20–22, 1994, IEEE Computer Society Press, pp. 124–134.

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA







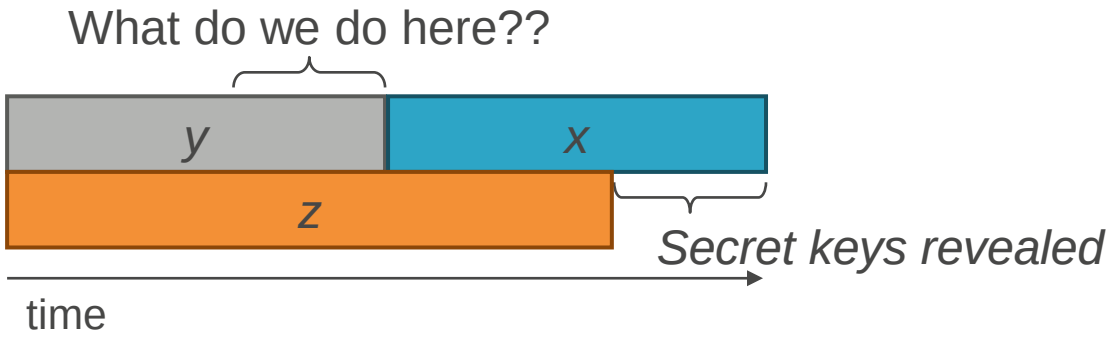
How much of a problem is quantum computing, really??

How soon do we need to worry?

Depends on:

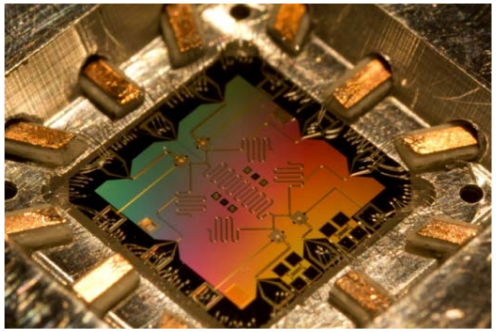
- How long do you need encryption to be secure? (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance? (*z* years)

Theorem 1: If $x + y > z$, then worry.

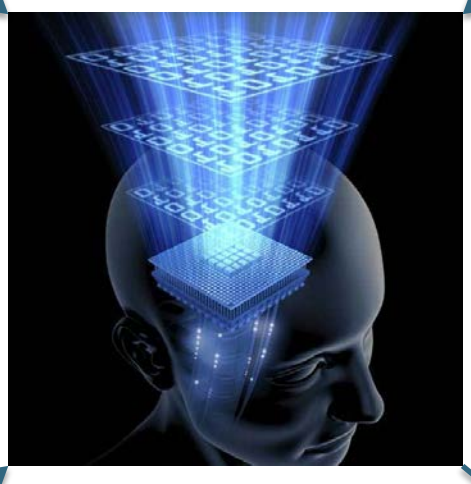


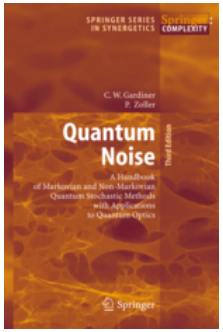
WHAT IS Z?

“Threshold theorem”



Architecture description





Error model

Threshold “ε”

If the error rates of the basic operations of the device are below ε,

then we can efficiently scale quantum computations.

What is ‘z’?

VOLUME 55, NUMBER 5, SEP./OCT. 2011
IBM Journal of Research and Development
Including IBM Systems Journal

Frontiers of Information Technology

M. Steffen
D. P. DiVincenzo
J. M. Chow
T. N. Theis
M. B. Ketchen

Quantum computing: An IBM perspective

Quantum physics provides an intriguing basis for achieving computational power to address certain categories of mathematical problems that are completely intractable with machine computation as we know it today. We present a brief overview of the current theoretical and experimental works in the emerging field of quantum computing. The implementation of a functioning quantum computer poses tremendous scientific and technological challenges, but current rates of progress suggest that these challenges will be substantively addressed over the next ten years. We provide a sketch of a quantum computing system based on superconducting circuits, which are the current focus of our research. A realistic vision emerges concerning the form of a future scalable fault-tolerant quantum computer.

formulated as experience is gained. We are still a long way from building a practical quantum computer, but the path toward this goal is becoming clearer.

Conclusion

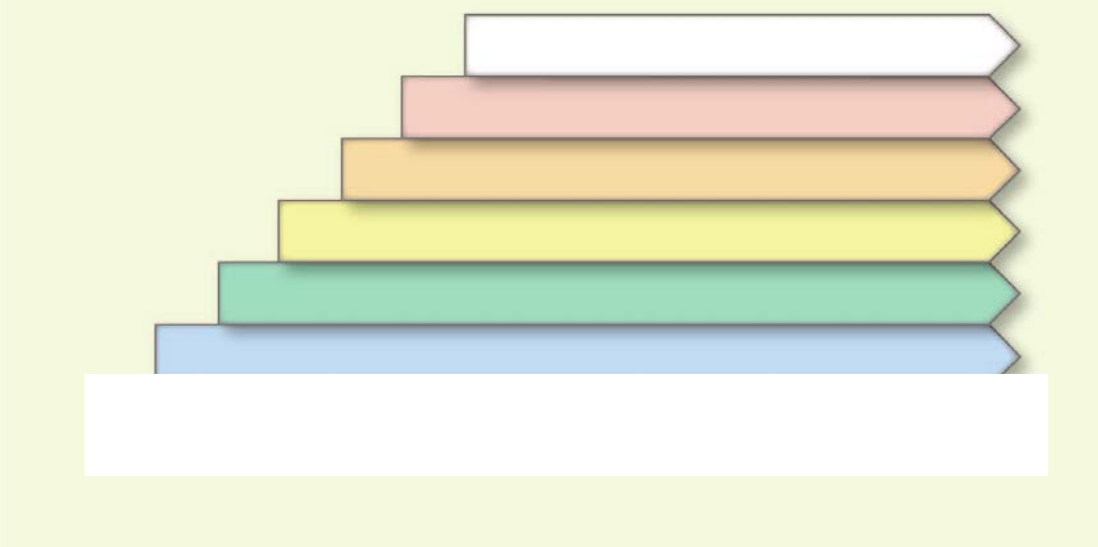
While we still have a long way to go and many details to work out, we can see the broad form of tomorrow's quantum computers. The marked progress in the theory of QEC has relaxed the device error rate that must be achieved for fault-tolerant computing. Rapid improvements in experimental quantum hardware suggest that a threshold for the design and the construction of fault-tolerant systems may be reached in the next five years. At that point, the goal of building a useful and reliable quantum computer will be within our reach.

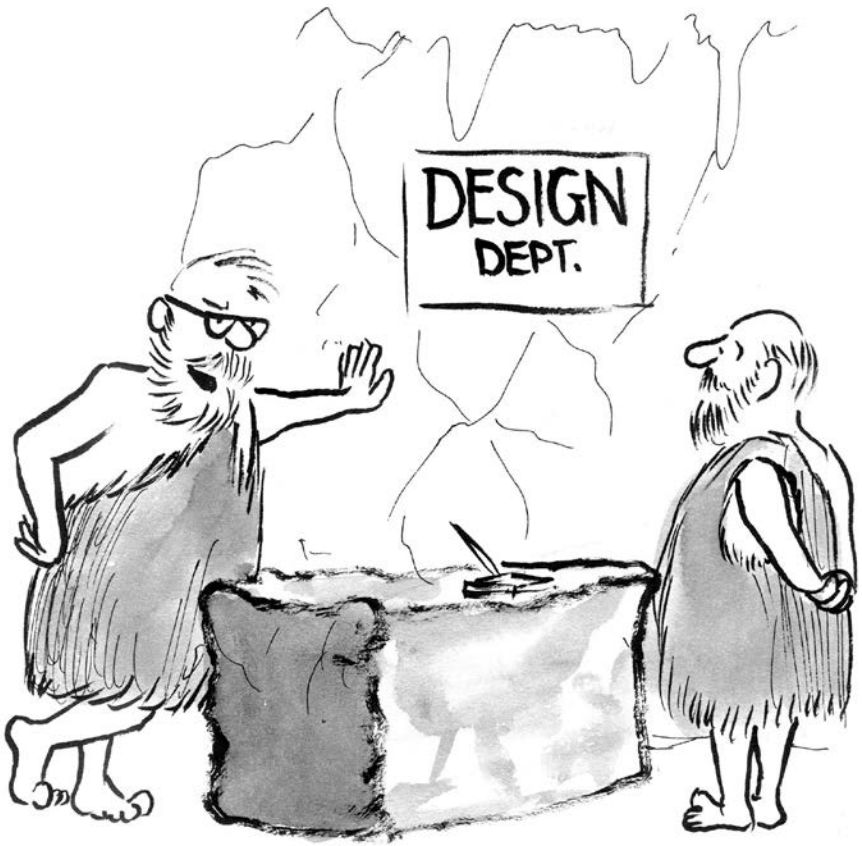
REVIEW

SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

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





"The wheel was great. What have you done for me lately?"

But what has happened lately?

Ongoing progress in quality of gates, readout, and the complexity of systems researchers are integrating.

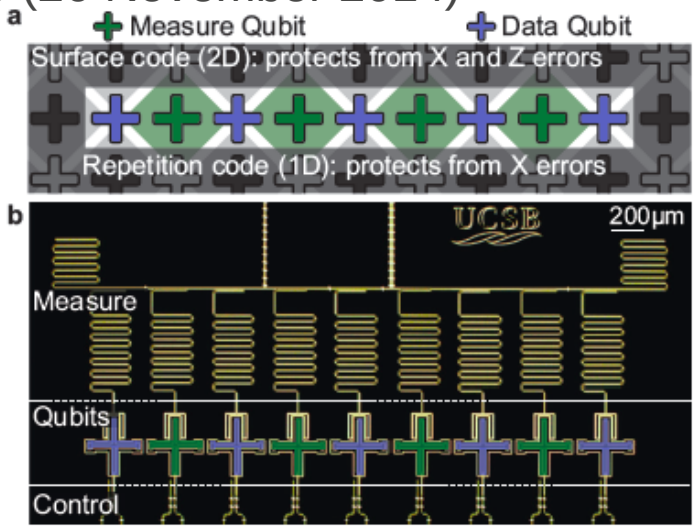
e.g.

State preservation by repetitive error detection in a superconducting quantum circuit

J. Kelly,[1,*] R. Barends,[1,2,*] A. G. Fowler,[1,3,2,*] A. Megrant,[1,4] E. Jeffrey,[1,2] T. C. White,[1] D. Sank,[1,2] J. Y. Mutus,[1,2] B. Campbell,[1] Yu Chen,[1,2] Z. Chen,[1] B. Chiaro,[1] A. Dunsworth,[1] I.-C. Hoi,[1] C. Neill,[1] P. J. J. O'Malley,[1] C. Quintana,[1] P. Roushan,[1,2] A. Vainsencher,[1] J. Wenner,[1] A. N. Cleland,[1] and John M. Martinis[1,2]

[1]*Department of Physics, University of California, Santa Barbara, CA 93106, USA*
[2]*Present address: Google Inc.*
[3]*Centre for Quantum Computation and Communication Technology, School of Physics, The University of Melbourne, Victoria 3010, Australia*
[4]*Department of Materials, University of California, Santa Barbara, CA 93106, USA*

arXiv:1411.7403 (26 November 2014)



Bottom-line:

Quantum computers capable of catastrophically breaking our public-key cryptography infrastructure are a *medium-term* threat.

Good news: we know how to fix it ….in theory

Worrisome news: there is a long road ahead

The solutions

Quantum-safe cryptographic infrastructure

“post-quantum” cryptography + **quantum cryptography**

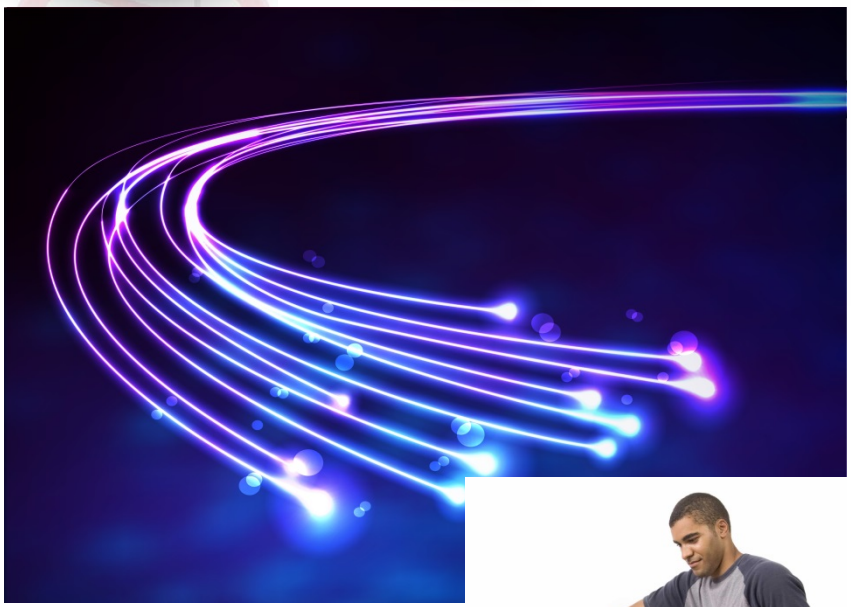
- classical codes deployable without quantum technologies
- believed/hoped to be secure against quantum computer attacks of the future

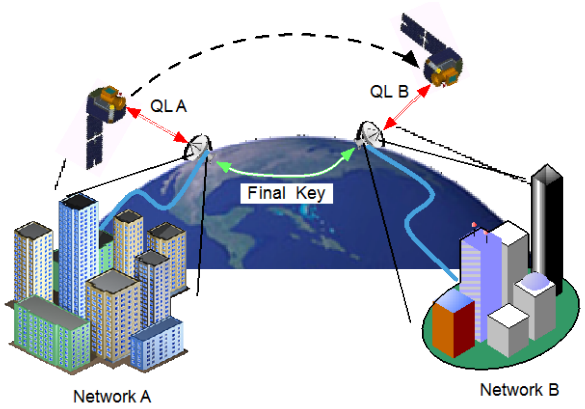
- quantum codes requiring some quantum technologies (typically less than a large-scale quantum computer)
- typically no computational assumptions and thus known to be secure against quantum attacks

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

The ultimate key-establishment tool (wrt security)

Quantum physics guarantees the security of the cryptographic key





A quantum satellite in LEO can interconnect ground networks located anywhere on Earth.

Together with ground-based repeaters, we will eventually have a “quantum internet”.

One advantage of quantum key-exchange combined with public-key signatures

Public-key encryption requires a “trapdoor predicate”.

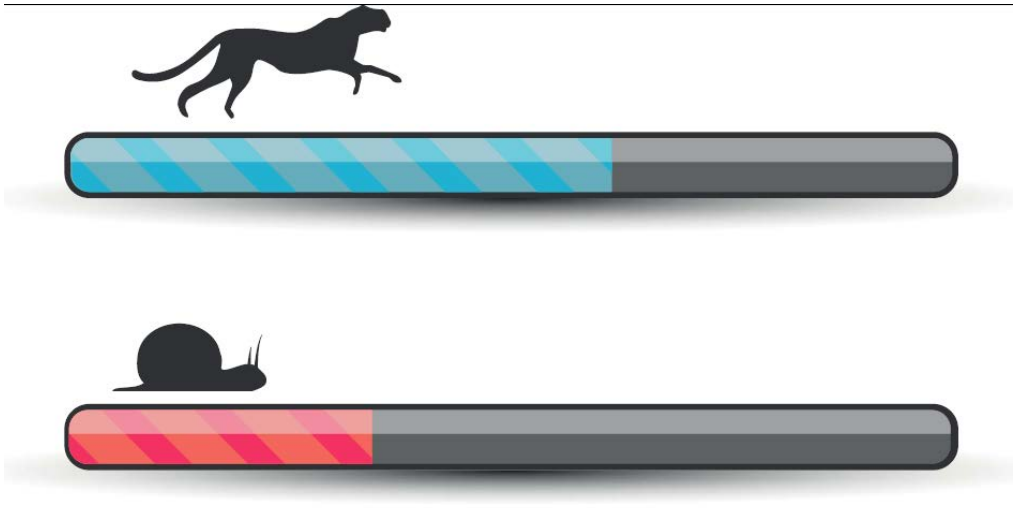
Signatures only require a “one-way function”.

- Few known potentially quantum-safe alternatives for PKE

- Many likely quantum-safe alternatives for OWF
- A big advantage of QKD is that it allows key establishment with public-key authentication, but does not need a trap-door predicate

What is ‘y’?

How long to quantum-proof?



Are there options? Are they quantum-safe?

Cryptographers are studying possible quantum-safe codes.

Quantum information experts are researching the power of quantum algorithms, and their impact on computationally secure cryptography.

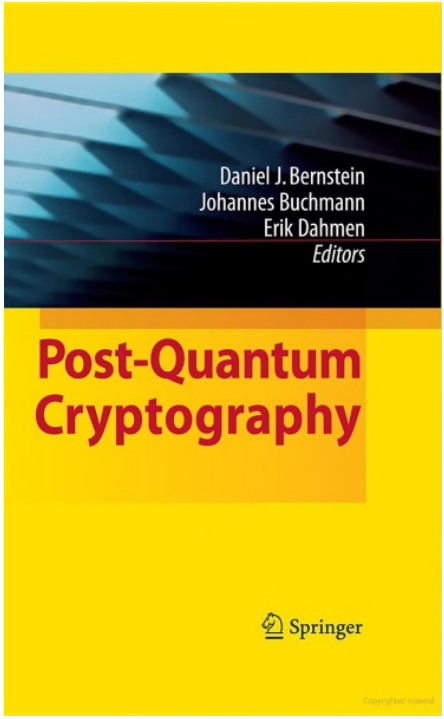
Lorentz center

Post-Quantum Cryptography and Quantum Algorithms

Workshop: 5 – 9 November 2012, Leiden, the Netherlands

SCHLOSS DAGSTUHL
Leibniz-Zentrum für Informatik

Sept. 18th - 23rd 2011,
Dagstuhl Seminar 11381
Sept. 8th - 13th 2013,
Dagstuhl Seminar 13371
***Sept. 7th – 11th* 2015**



PQCrypto 2013, 4th to 7th of June - Limoges, France

Fifth International Conference on Post-Quantum Cryptography

PQCrypto 2014 1-3 October, 2014, Waterloo, Canada

6TH INTERNATIONAL CONFERENCE ON POST-QUANTUM CRYPTOGRAPHY

Seventh International Conference on Post-Quantum Cryptography

PQCrypto 2016

Fukuoka, Japan, February 24–26, 2016

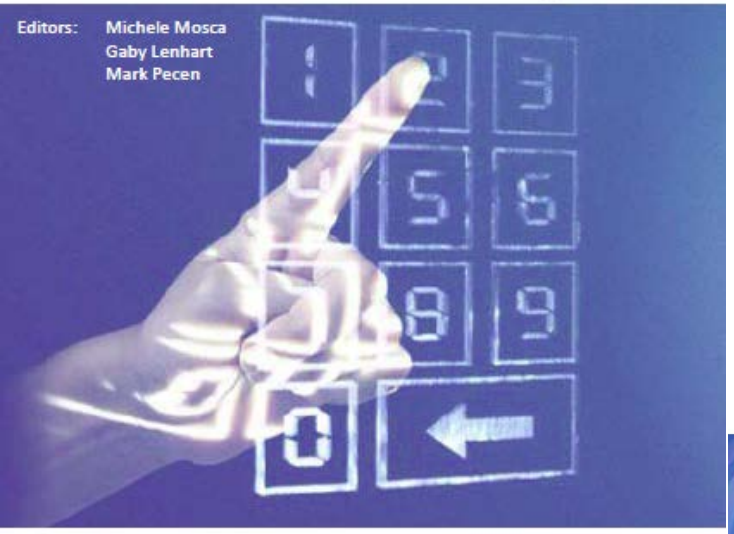
https://pqcrypto2016.jp/

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

CryptoWorks21

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

Are the standards and practices ready?



Workshop on Cybersecurity in a Post-Quantum World, 2-3 April 2015

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

Is the workforce ready?

Security is a choice

Overcoming obstacles to quantum-proofing

Challenges

- Performance
- Battle-testing:
  - Implementation errors
  - Protocol errors
  - Side-channel attacks
  - etc
- Availability
- Resistance to improving something that currently works
- Interoperability and standardization

Potential approaches

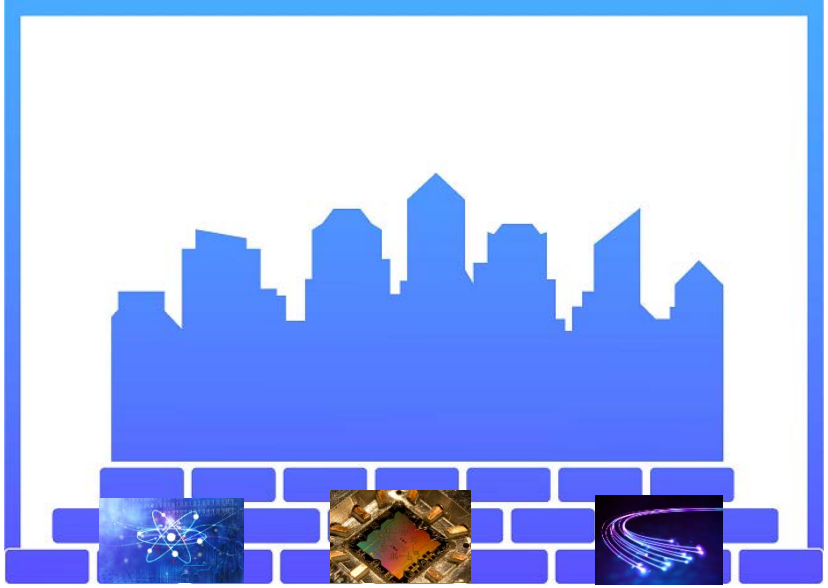
- Benchmarking/challenges
- Hybridize conventional signatures and key establishment with quantum-safe signatures and key establishment
- Offer open-source reference implementations
- Engage in dialogue with standards organizations, white-papers, etc.

Suggestions for Industry and Government

- Get quantum-safe options on vendor roadmaps
  - Routinely ask about vulnerability of systems to quantum attacks
  - Include quantum-safe options as desired features
  - Keep switching costs low
- (If appropriate) request the necessary standards for the quantum-safe tools needed
- Request the information/studies needed to make wise decisions going forward
- Applaud and reward organizations that take this seriously.

Suggestions for Individuals

- Tell organizations responsible for protecting your information that:
  - you are concerned about your information being compromised when quantum computers arrive.
  - you are concerned about the broader economic and social impact of their systems not being quantum-safe in time.
  - you'd like to know more about what they are doing to prepare for this.
- Applaud and reward organizations that take this seriously.



Quantum mechanics forces us to reinvent the foundations of our cryptographic infrastructure.

Quantum-safe is a necessary condition to be cyber-safe

We need to take advantage of the head-start we have been given, and make the next generation ICT infrastructure as secure and robust as we can.

The planning needs to start ***now***.

Thank you!

- Feedback welcome: mmosca@uwaterloo.ca