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

QCrypt 2015

Tokyo

Michele Mosca

2 October 2015

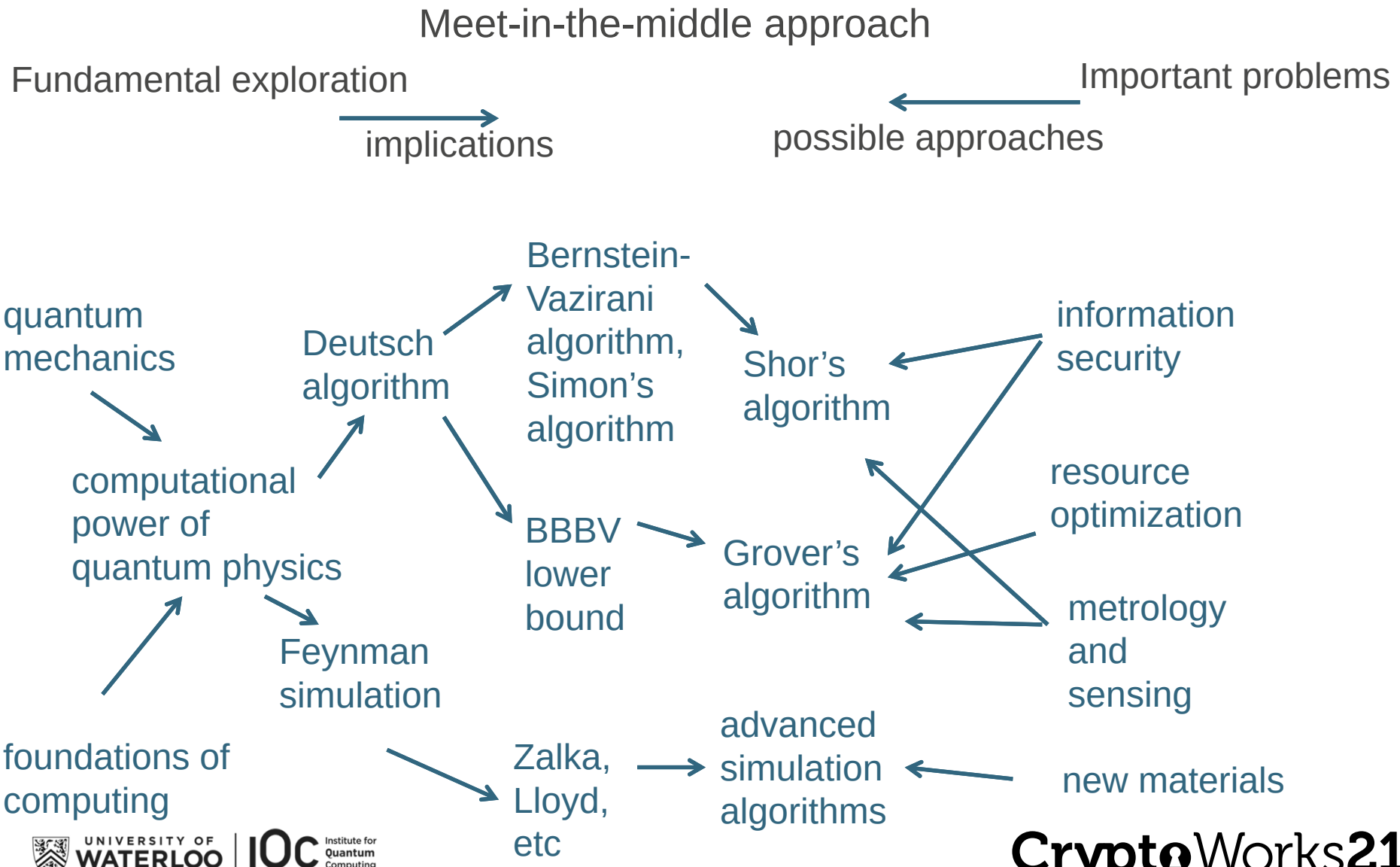
PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

evolution

CryptoWorks21

The search for high-impact discoveries



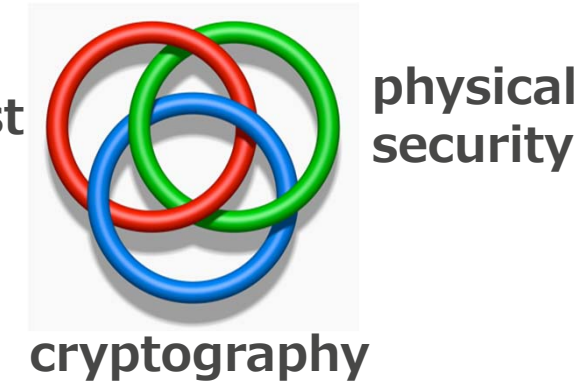
Cyber technologies are increasingly pervasive.

NUCLEAR POWER STATION

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.



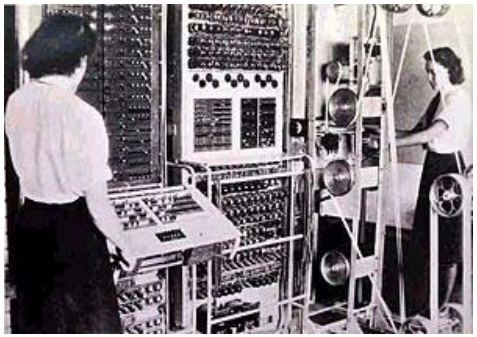
e.g. Do you update your software and anti-virus daily? Why do you trust the source?

(recall Buchmann talk this morning)
N.B. Cryptography is susceptible to "record now, decrypt later".

Some of the computational assumptions underlying cryptography are occasionally broken.

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



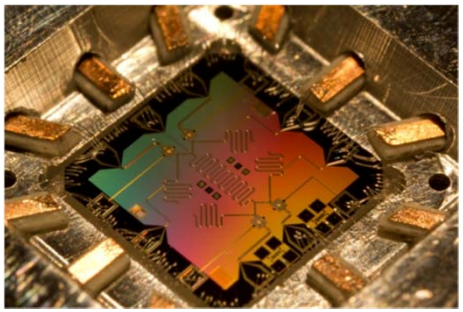
Prof. Bill Tutte was responsible for cracking these codes (see http://math.uwaterloo.ca/combinatorics-and-optimization/about/professor-william-t-tutte for more information). In 1943, the electronic computer COLOSSUS was designed and built by the British Post Office in order to run the algorithms that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

…An unexpected threat to cybersecurity:
a new paradigm for physics and computation!

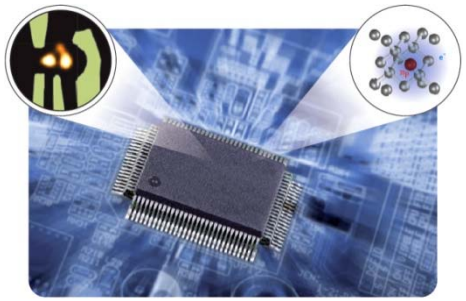
Algorithms for Quantum Computation:
Discrete Logarithms and Factoring

Peter W. Shor

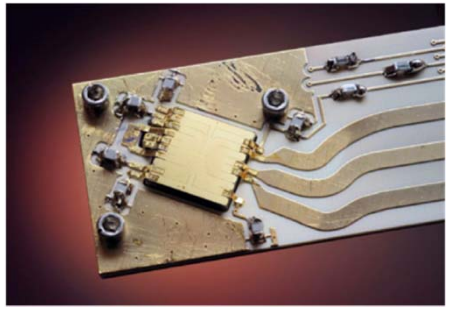
In Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20-22, 1994, IEEE Computer Society Press, pp. 124-134.



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



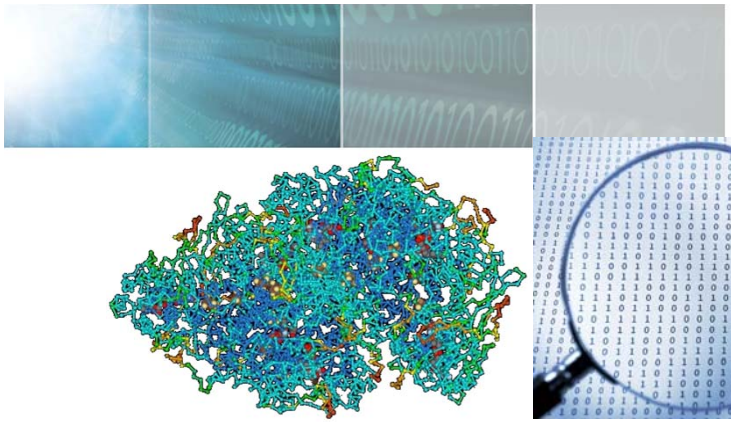
Christian Lagerek/Alamy



Y. Colombe/NIST

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."

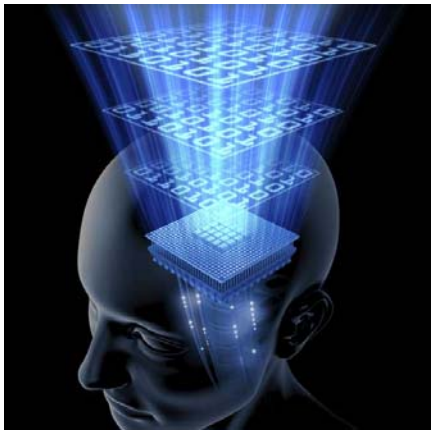


Simulating quantum mechanical systems

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…

For the advent of large-scale quantum computation to be a positive milestone in human history, **we must first make our cryptographic infrastructure secure against quantum attacks.**

A historical fluke/opportunity

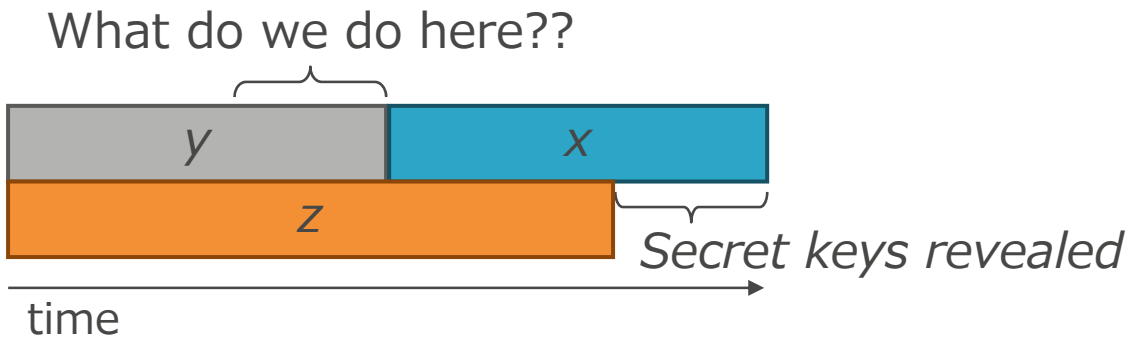
- Our current crypto infrastructure is not nearly as good as it could be.
- In practice it is nearly impossible to replace something "good enough" with something better.
- Given that we have no choice but to replace fundamental cryptography tools with something quantum-safe, the **"toolbox" must be opened.**
- Now is a critical time to design the "better" tools and practices into the next generation cryptographic infrastructure before the toolbox is effectively shut again.
- This also means that systems-level research of new quantum-safe tools (both QKD and post-quantum) is needed *now.*

How soon do we need to worry?

Depends on:

- How long do you need your keys 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.



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.

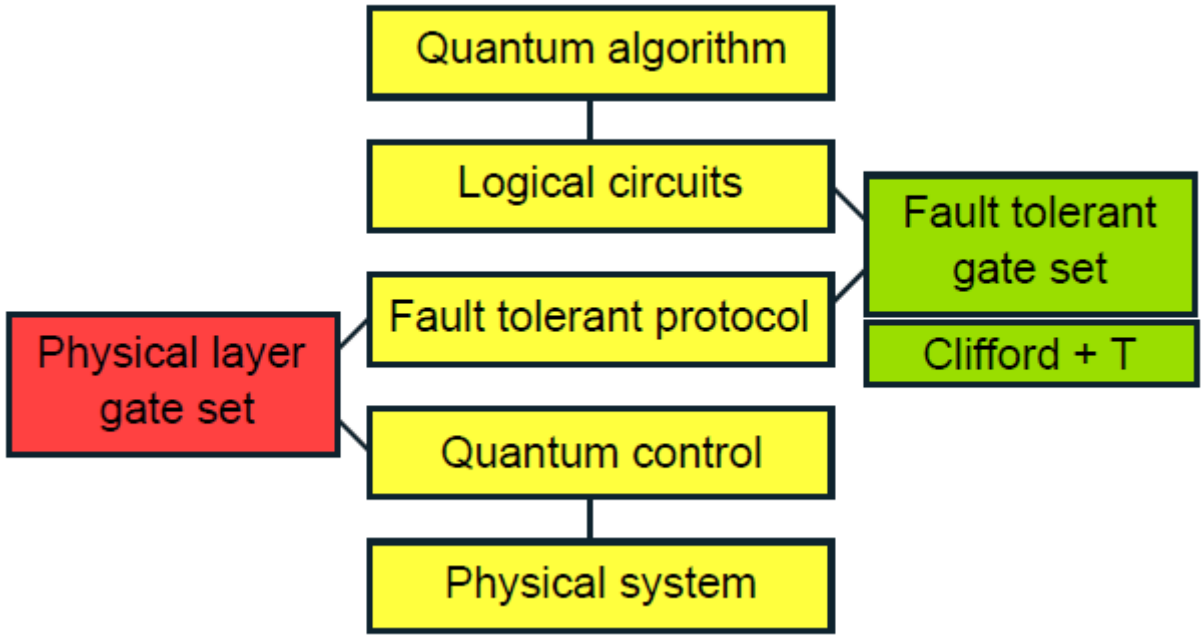
- **Prediction:** In the next 6-24 months, organizations without a well-articulated quantum risk management plan will lose business to organizations that do.

WHAT IS Z?

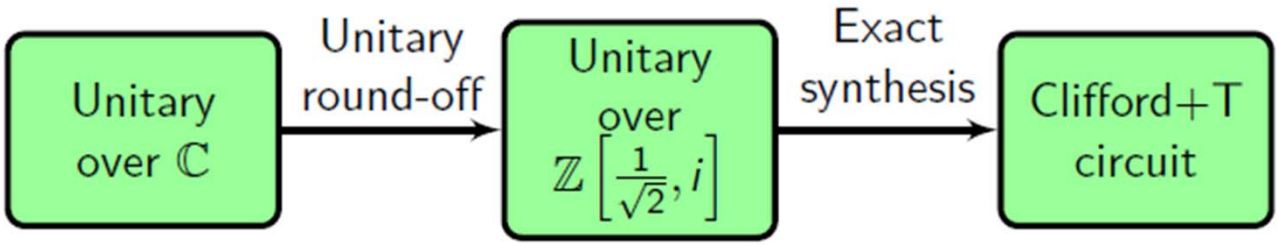
What resources are required to break RSA-2048?

- A billion physical qubits and a trillion physical gates?
- A million qubits and 100 million gates?
- Something else?
- Asymptotic complexity estimates give a very coarse-grained approximation.
- To attempt to estimate this question, we need a more fine-grained study of the full tool chain between algorithms and physical qubits.

Quantum compilers



Examples:



- Use number theory methods to bypass Solovay-Kitaev algorithm and achieve optimal synthesis of one-qubit unitaries (over Clifford and T gates)
- Use matroid partitioning to reduce T-complexity and T-depth
- Use channel representation of unitaries to find optimal T-depth

When will we have those resources?

REVIEW

SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

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

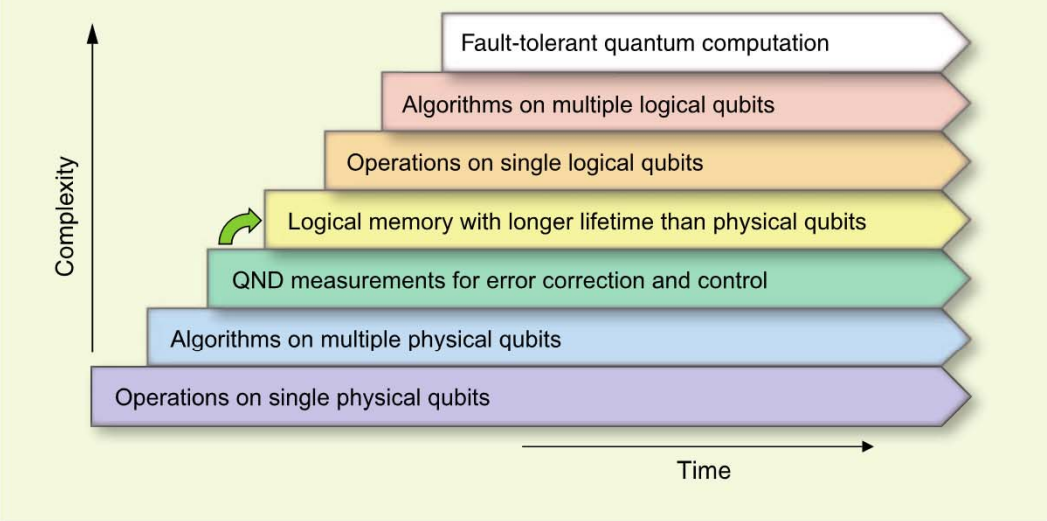


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third 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.

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

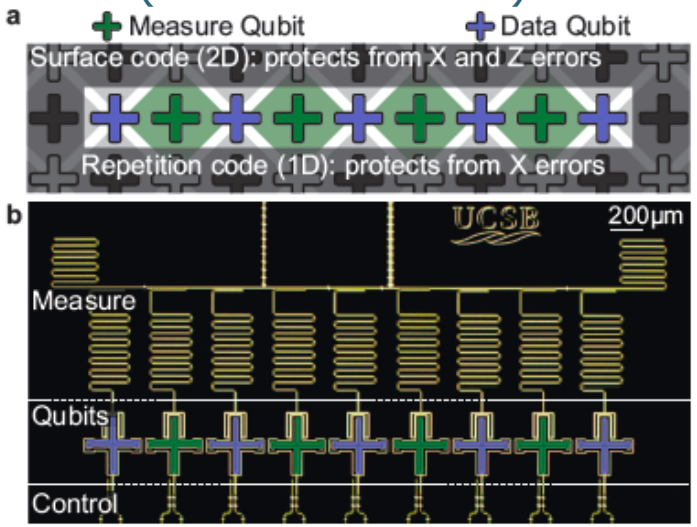
e.g.

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*

Nature 519, 66–69 (05 March 2015) doi:10.1038/nature14270



MM:
[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"

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."*

NSA [August 2015]: *NSA's Information Assurance Directorate "will initiate a transition to quantum resistant algorithms in the not too distant future."*

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

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

+ quantum cryptography

- quantum cryptographic tools 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

Terminology

"Quantum-safe"

=

"safe in the era with large-scale quantum computers"

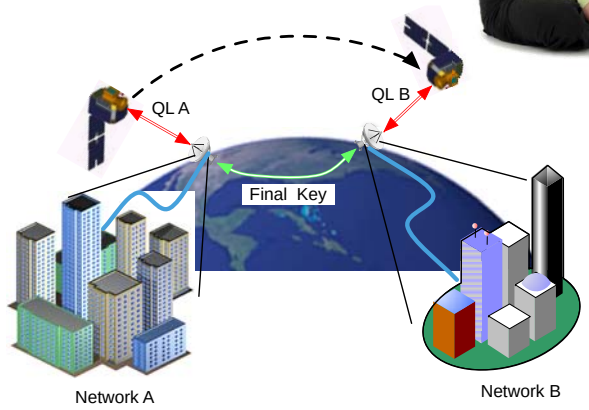
=

conventional "post-quantum"/ "quantum-resistant" cryptography

+ quantum cryptography

The ultimate key-establishment tool

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”.

Will QKD be a serious part of the next generation crypto infrastructure?

Some common objections to using QKD:

- Objection 1:
  - Just use post-quantum (classical) Public Key Encryption
- Objection 2:
  - Just use One-Way Function based crypto (Since QKD with information theoretically secure authentication can be viewed as key expansion)
- Objection 3:
  - Seeding a symmetric system (if using *e.g.* Wegman-Carter authentication) is as hard as Out-Of-Band key establishment
- Objection 4:
  - QKD today is essentially Out-Of-Band (Since it is not a transparent part of the existing global telecommunications systems)

Responses in:

A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys

Lawrence M. Ioannou[1,2] and Michele Mosca[1,2,3]
[1]*Institute for Quantum Computing, University of Waterloo, 200 University Avenue, Waterloo, Ontario, N2L 3G1, Canada*
[2]*Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue, Waterloo, Ontario, N2L 3G1, Canada*
[3]*Perimeter Institute for Theoretical Physics 31 Caroline Street North, Waterloo, Ontario, N2L 2Y5, Canada*

We give new arguments in support of *signed quantum key establishment*, where quantum cryptography is used in a public-key infrastructure that provides the required authentication. We also analyze more thoroughly than previous works the benefits that quantum key establishment protocols have over certain classical protocols, motivated in part by the various objections to quantum key establishment that are sometimes raised. Previous knowledge of quantum cryptography on the reader's part is not required for this article, as the definition of "quantum key establishment" that we use is an entirely classical and black-box characterization (one need only trust that protocols satisfying the definition exist).

Comments on objection 1

- Long-term secure public-key encryption is a highly optimistic assumption

- Short/medium term secure public-key encryption is a more realistic assumption
  - May be suitable where long term security of keys is not important
  - However, an unexpected break of a deployed public-key cryptosystem compromises the stability of a cryptographic infrastructure
    - Can we diversify and have already-deployed alternatives in order to maintain functionality and stability?
  - But what about when long-term confidentiality is needed?
    - *e.g.* http://eprint.iacr.org/2012/449

- One advantage of quantum key-exchange combined with public-key signatures http://arxiv.org/abs/1109.3235 (with Ioannou)

Public-key encryption requires a "trapdoor predicate".

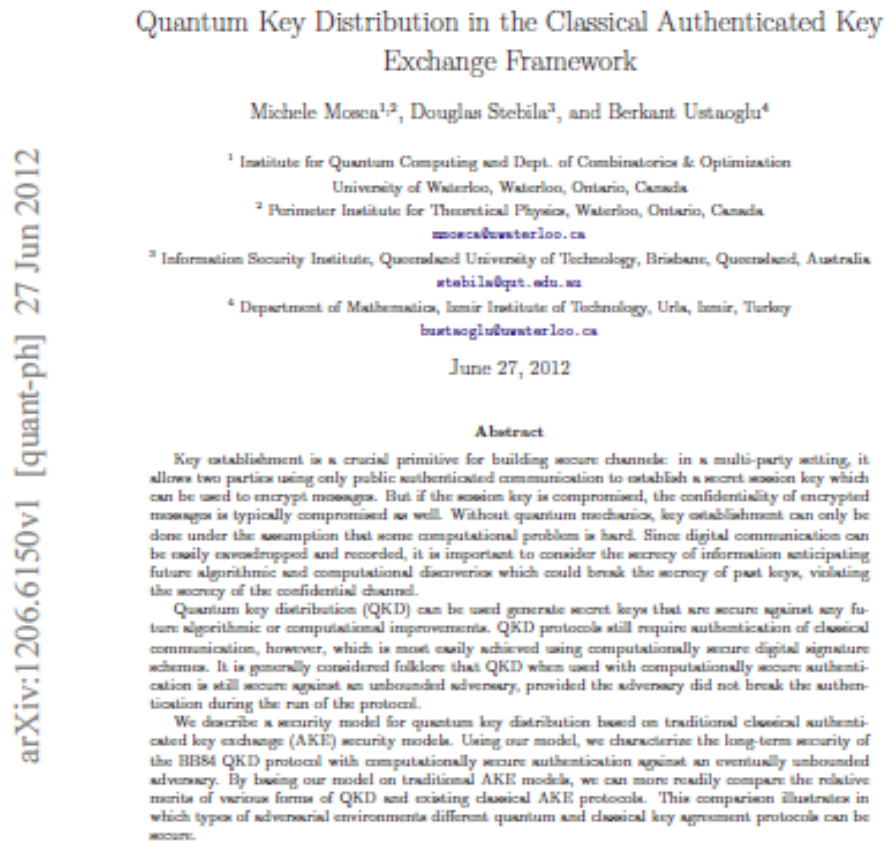
Signatures only require a "one-way function".

- 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

Other comments

- How resilient are some of these alternatives to



arXiv:1206.6150v1 [quant-ph] 27 Jun 2012

Quantum Key Distribution in the Classical Authenticated Key Exchange Framework

Michele Mosca[1,2], Douglas Stebila[3], and Berkant Ustaoglu[4]

[1] Institute for Quantum Computing and Dept. of Combinatorics & Optimization
University of Waterloo, Waterloo, Ontario, Canada
[2] Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada
mosca@uwaterloo.ca
[3] Information Security Institute, Queensland University of Technology, Brisbane, Queensland, Australia
stebila@qut.edu.au
[4] Department of Mathematics, Izmir Institute of Technology, Urla, Izmir, Turkey
bustaoglu@uwaterloo.ca

June 27, 2012

Abstract

Key establishment is a crucial primitive for building secure channels: in a multi-party setting, it allows two parties using only public authenticated communication to establish a secret session key which can be used to encrypt messages. But if the session key is compromised, the confidentiality of encrypted messages is typically compromised as well. Without quantum mechanics, key establishment can only be done under the assumption that some computational problem is hard. Since digital communication can be easily eavesdropped and recorded, it is important to consider the secrecy of information anticipating future algorithmic and computational discoveries which could break the secrecy of past keys, violating the secrecy of the confidential channel.

Quantum key distribution (QKD) can be used generate secret keys that are secure against any future algorithmic or computational improvements. QKD protocols still require authentication of classical communication, however, which is most easily achieved using computationally secure digital signature schemes. It is generally considered folklore that QKD when used with computationally secure authentication is still secure against an unbounded adversary, provided the adversary did not break the authentication during the run of the protocol.

We describe a security model for quantum key distribution based on traditional classical authenticated key exchange (AKE) security models. Using our model, we characterize the long-term security of the BB84 QKD protocol with computationally secure authentication against an eventually unbounded adversary. By basing our model on traditional AKE models, we can more readily compare the relative merits of various forms of QKD and existing classical AKE protocols. This comparison illustrates in which types of adversarial environments different quantum and classical key agreement protocols can be secure.

Is QKD "out-of-band"?
i.e. comparable to trusted courier?

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

Bottom line

In some cases, QKD adds significant value, in other cases it doesn't.

Users can decide if it adds value for them, and if the costs justify the benefits.

QKD would definitely add value to the overall cryptographic infrastructure, especially as QKD technology advances.

However, we can't take for granted that QKD will be adopted as widely as it could/should.

Existing detailed analyses

K. G. Paterson, F. Piper, and R. Schack (2004)

"Quantum cryptography: a practical information security perspective" (formerly, "Why quantum cryptography?")

Published in Quantum Communication and Security, Proceedings, NATO Advanced Research Workshop, edited by M. Zukowski S. Kilin and J. Kowalik, p. 175-180 (IOS Press, Amsterdam, 2007) http://arxiv.org/abs/quant-ph/0406147

R. Alleaume, *et al.* (2007)

"SECOQC white paper on quantum key distribution and cryptography" http://arxiv.org/abs/quant-ph/0701168

D. Stebila, M. Mosca, and N. Lütkenhaus (2009)

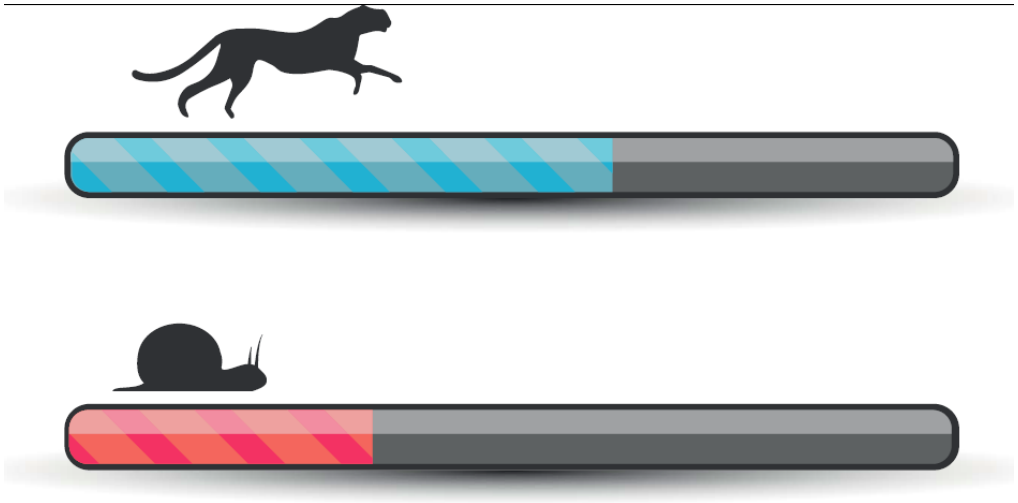
"The case for quantum key distribution"

Proceedings of QuantumComm 2009 Workshop on Quantum and Classical Information Security, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, volume 36, page 283--296. Springer, 2010.

- D. Bernstein (2009)
  - "Cost-benefit analysis of quantum cryptography" http://www.dagstuhl.de/Materials/index.en.phtml?09311
- S. Kunz-Jacques and P. Jouquet (2011)
  - "Using hash-based signatures to bootstrap quantum key distribution" http://arxiv.org/abs/1109.2844
- L. Ioannou and M. Mosca (2011)
  - "A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys" http://arxiv.org/abs/1109.3235
- M. Mosca, D. Stebila, and B. Ustaoglu (2012)
  - "Quantum key distribution in the classical authenticated key exchange framework http://arxiv.org/abs/1206.6150

What is ‘y’?

How long to quantum-proof?



Are the post-quantum options really quantum-safe?

Cryptographers are studying possible quantum-safe codes.

We need quantum algorithms experts to study the power of quantum algorithms, and their impact on computationally secure cryptography.

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

Is the workforce ready?

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

Are the standards and practices ready?

Are the standards and practices ready?

IETF

NIST National Institute of Standards and Technology U.S. Department of Commerce

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

NICT National Institute of Information and Communications Technology

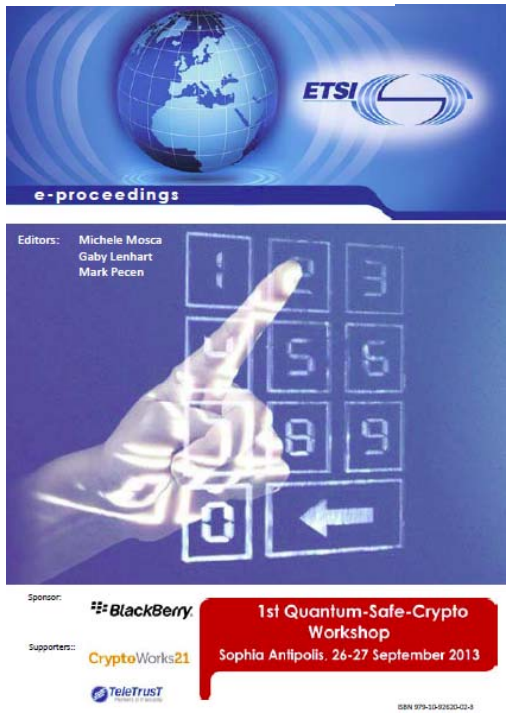
ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges

June 2015

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



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
5-7 October, 2015, Seoul, Korea

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

CryptoWorks21

Security is a choice

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
- Make quantum risk management a part of their cybersecurity roadmap
- (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-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.

We need industry and government to decide to make cyber-systems quantum-safe.

There are many important research challenges to be tackled to get us there!

Thank you!

Feedback welcome: mmosca@iqc.ca

Canada Foundation for Innovation

Fondation canadienne pour l'innovation

evolution

CIFAR
CANADIAN INSTITUTE FOR ADVANCED RESEARCH

CryptoWorks21

Canada