Title: PSI 2016/2017 Quantum Information (Review) - Lecture 12 (Michele Mosca)

Date: Mar 09, 2017 02:00 PM

URL: http://pirsa.org/17030036

Abstract:

Generalization: Amplitude Amplification
(BBHT,BH,BHT,G,BHMT,…)

$$A|0\rangle = |\Psi\rangle \qquad |\Psi\rangle = \sin(\theta)|\Psi_1\rangle + \cos(\theta)|\Psi_0\rangle$$

$$Q = -AU_0A^{-1}U_f$$

$$Q^k A|0\rangle = \sin((2k+1)\theta)|\psi_1\rangle + \cos((2k+1)\theta)|\psi_0\rangle$$

We need

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2} \approx O\left(\frac{1}{\sqrt{p}}\right)$$

74

Non-trivial applications of Amplitude Amplification

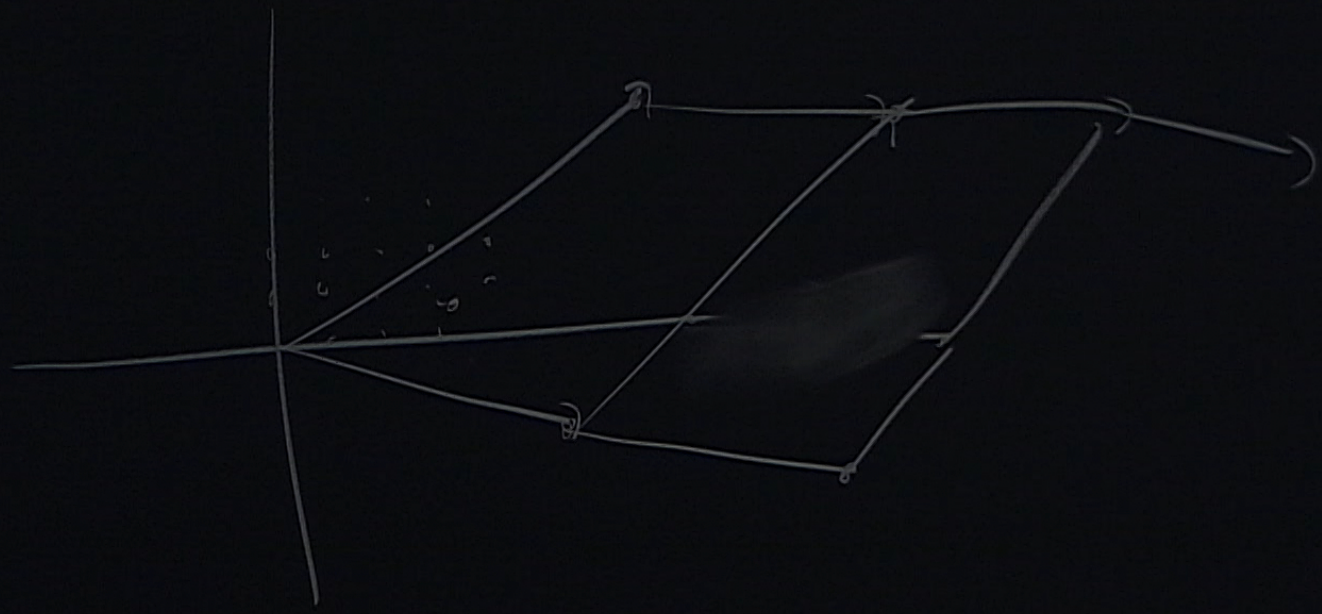
For example…

- Minimum/maximum finding
- Collision-finding
- String-matching
- Making quantum algorithms “exact”
- Several graph problems
- Etc. etc.

$\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$

$f(\vec{x}) = f(\vec{y})$

$\Leftrightarrow \vec{x} - \vec{y} \in L$



Generalizations of Abelian HSP

- Can view HSP has a hidden sub-lattice problem for $Z \otimes Z \otimes \cdots \otimes Z = Z^n$.

  One way to generalize the problem, is to find a hidden sub-lattice of $R \otimes R \otimes \cdots \otimes R = R^n$.

  Need to define appropriate ways for specifying/approximating inputs and outputs.

  Applications include solving Pell's equation, Principal Ideal Problem, and finding the unit group of a number field.

Generalizations of Abelian HSP

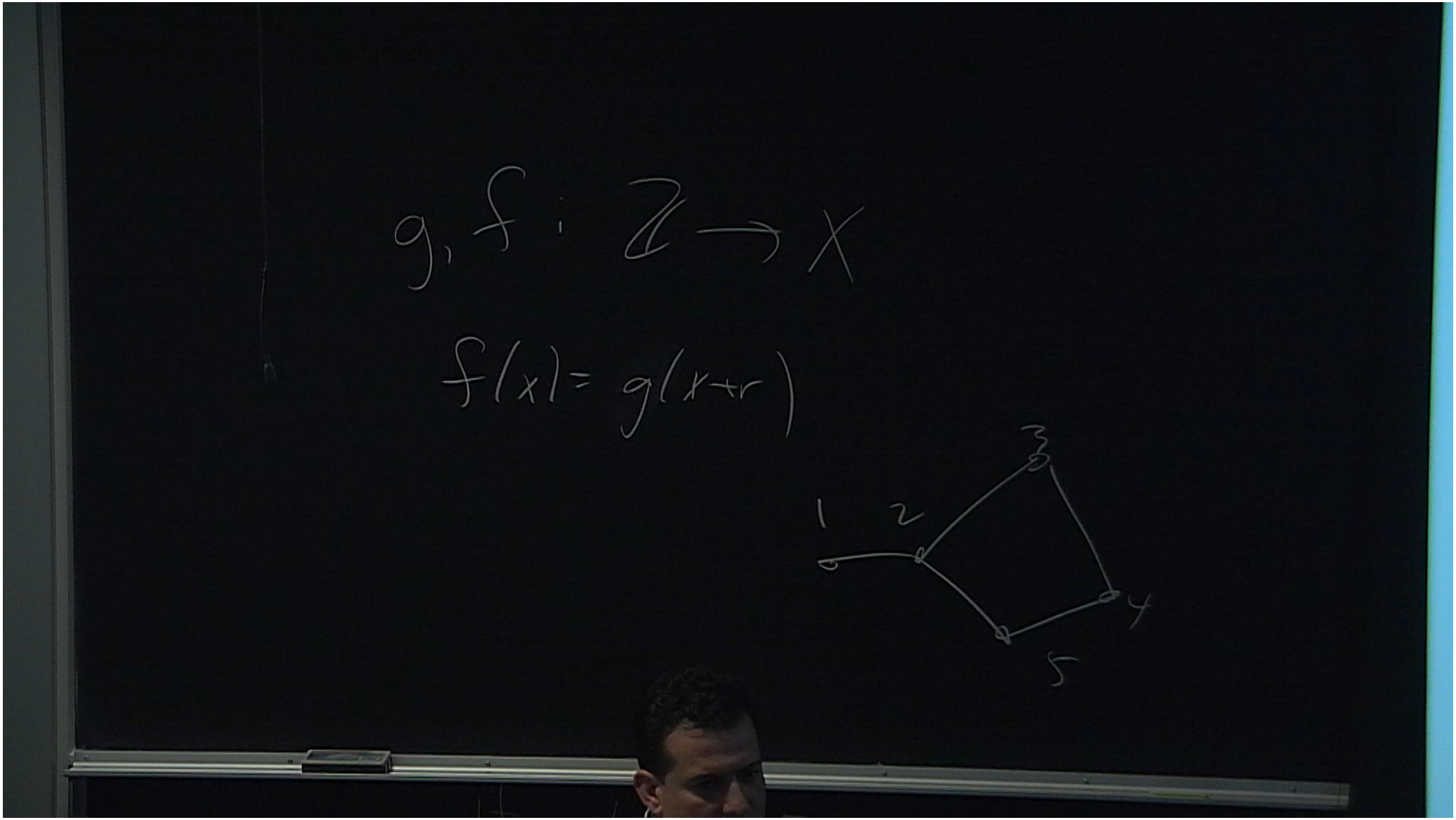
- Finding Hidden Shifts and Translations
- Can generalize to finding hidden “non-linear” structures. E.g. hidden radius problem, shifted subset problem, hidden polynomial problem
- Estimating “Gauss sums”
- Etc.

Quantum walk algorithms

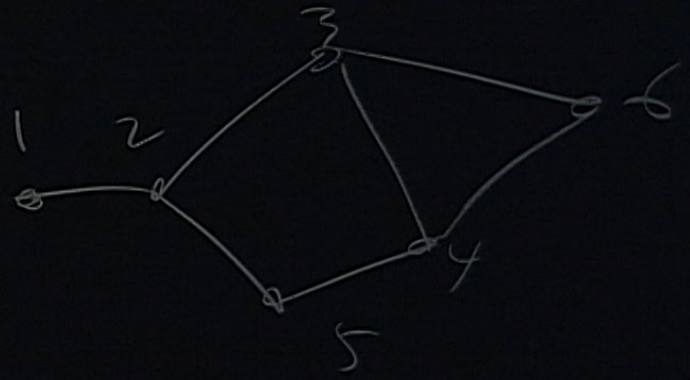
- Can generalize notion of classical random walks
- Can get up to quadratic speed-up for "mixing time"
- Can get up to an exponential speed-up for "hitting time" ("glued-trees" problem)

- For discrete-time versions, it is usually necessary to add a "coin".
- Applications include:

Element distinctness, triangle-finding, element k-distinctness, AND-
OR trees, MIN-MAX trees, etc.


g, f : Z → X
f(x) = g(x+r)
1
2
3
4
5

$f(x) = g(x+r)$



Using adiabatic theorem for computation (Farhi et al.)

- H_0 - easy to compute ground state.
- H_1 - ground state is solution to some problem.
- H_0 and H_1 can both be efficiently implemented.

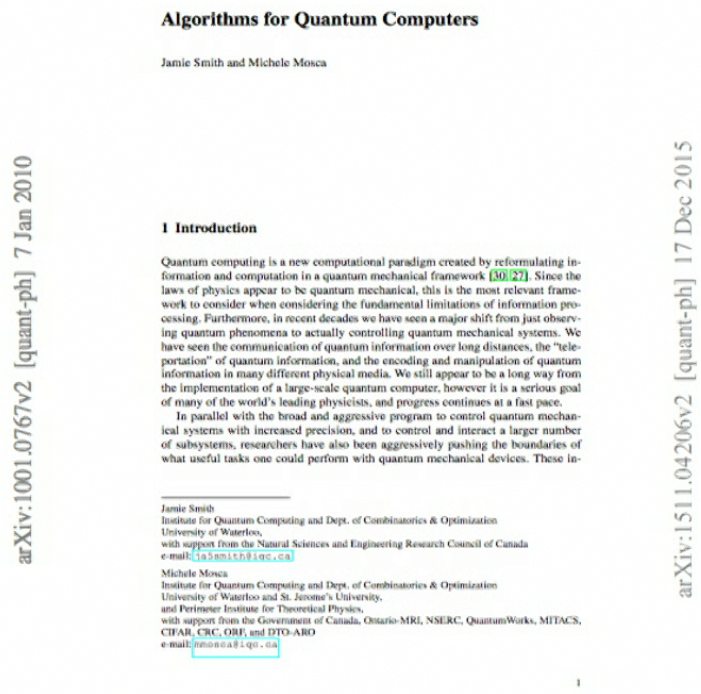
92

Algorithms for quantum tasks

- Other quantum transformations (e.g. Clebsch-Gordan, wavelet)
- Generating general quantum states
- Quantum error correction
- Quantum signature schemes
- Quantum data compression
- Quantum entanglement concentration
- Coset orbit problem
- Etc. etc.

94

Further reading



Algorithms for Quantum Computers

Jamie Smith and Michele Mosca

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

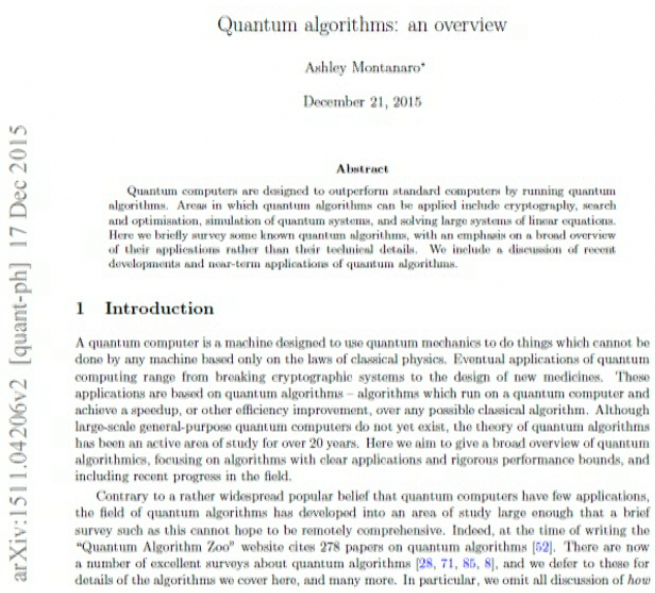
1 Introduction

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



Quantum algorithms: an overview

Ashley Montanaro*

December 21, 2015

arXiv:1511.04206v2 [quant-ph] 17 Dec 2015

Abstract

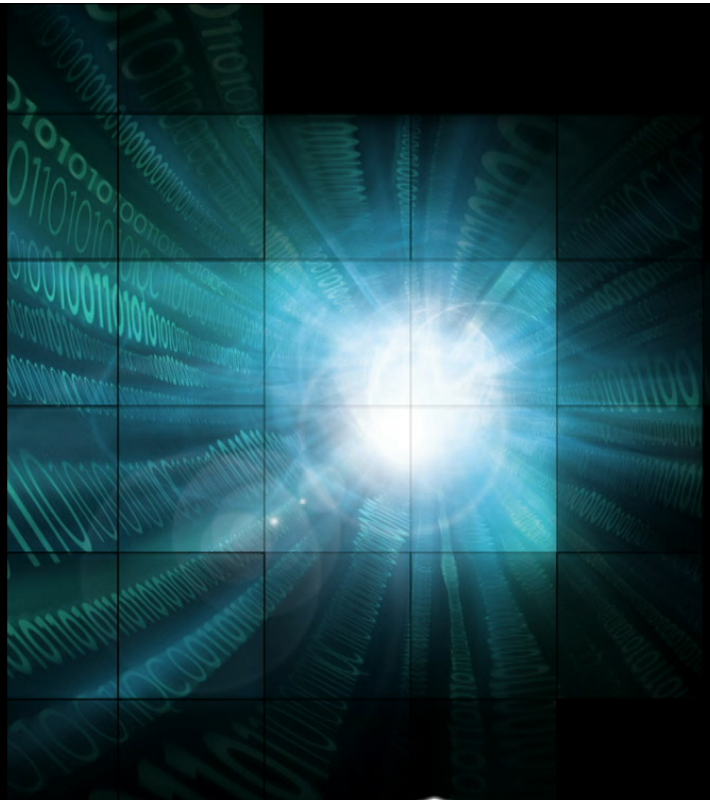
Quantum computers are designed to outperform standard computers by running quantum algorithms. Areas in which quantum algorithms can be applied include cryptography, search and optimisation, simulation of quantum systems, and solving large systems of linear equations. Here we briefly survey some known quantum algorithms, with an emphasis on a broad overview of their applications rather than their technical details. We include a discussion of recent developments and near-term applications of quantum algorithms.

1 Introduction

A quantum computer is a machine designed to use quantum mechanics to do things which cannot be done by any machine based only on the laws of classical physics. Eventual applications of quantum computing range from breaking cryptographic systems to the design of new medicines. These applications are based on quantum algorithms – algorithms which run on a quantum computer and achieve a speedup, or other efficiency improvement, over any possible classical algorithm. Although large-scale general-purpose quantum computers do not yet exist, the theory of quantum algorithms has been an active area of study for over 20 years. Here we aim to give a broad overview of quantum algorithmics, focusing on algorithms with clear applications and rigorous performance bounds, and including recent progress in the field.

Contrary to a rather widespread popular belief that quantum computers have few applications, the field of quantum algorithms has developed into an area of study large enough that a brief survey such as this cannot hope to be remotely comprehensive. Indeed, at the time of writing the "Quantum Algorithm Zoo" website cites 278 papers on quantum algorithms [52]. There are now a number of excellent surveys about quantum algorithms [28, 71, 85, 8], and we defer to these for details of the algorithms we cover here, and many more. In particular, we omit all discussion of *how*

http://math.nist.gov/quantum/zoo/



Cybersecurity in a Quantum World: will we be ready?

Perimeter Scholars International

Michele Mosca
mmosca@perimeterinstitute.ca
mmosca@uwaterloo.ca

9 February 2017

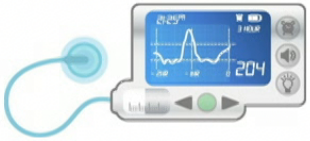
PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

CryptoWorks21

Cyber technologies are becoming increasingly pervasive



evolution

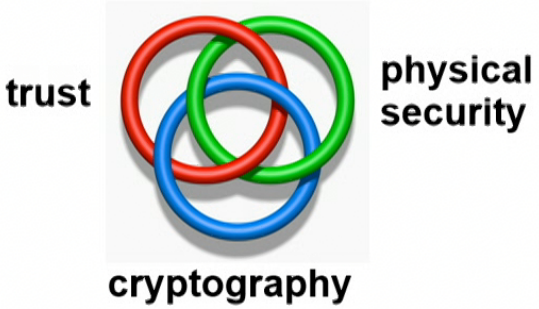
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Cybersecurity

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.



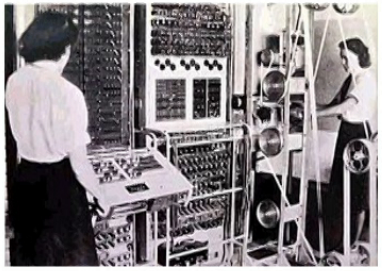
e.g. Do you update your software and anti-virus daily? Why do you trust the source?

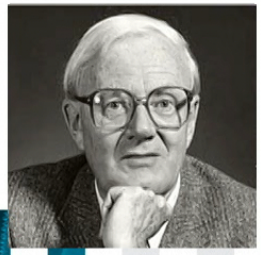
N.B. Cryptography is susceptible to “record now, decrypt later”.

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.

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Recent Developments in Cryptanalysis of Public-Key Cryptosystems

Alfred Menezes

University of Waterloo

https://docbox.etsi.org/Workshop/2016/201609_QUANTUMSAFECRYPTO/TECHNICAL_TRACK/UniversityofWaterloo_Menezes.pdf

Symmetric Pairings Disaster

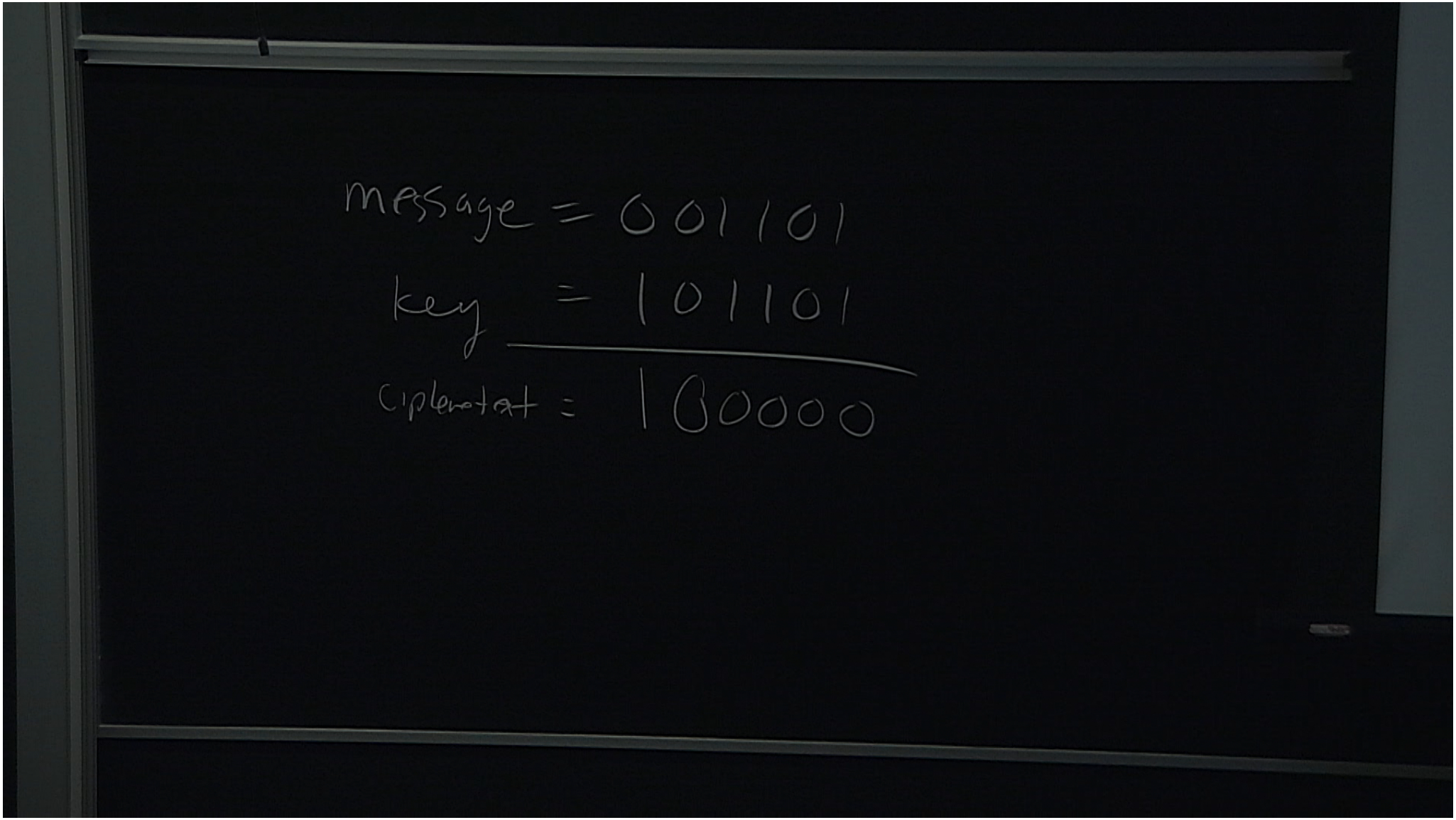
- 2013: Joux: $L_Q[\frac{1}{4} + o(1), c]$ algorithm for DLP in $\mathbb{F}_{2^{4m}}$ and $\mathbb{F}_{3^{6m}}$.
- 2013: Barbulescu et al.: Quasi-polytime $L_Q[\epsilon, c]$ algorithm ($\epsilon > 0$).
- 2016: Adj et al.:
  - Computed discrete logs in the 4841-bit field $\mathbb{F}_{3^{6 \cdot 509}}$ in 220 CPU years.
  - This field provides 128 bits of security against Coppersmith's attack.
  - Estimated that discrete logs in the 13590-bit field $\mathbb{F}_{3^{6 \cdot 1429}}$ can be computed in 3000 CPU years.
  - This field provides 192 bits of security against Coppersmith's attack.

Lessons Learned

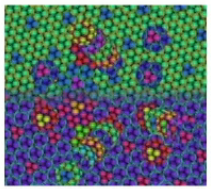
- Passage of time is not a strong argument for security unless the underlying hard problem indeed has been intensively studied by many experts.
- One can get a false sense of security when hundreds of protocols papers are written with claims of "provable security".
- Example: LWE, RLWE
  - Extensively used to design cryptographic protocols since Regev proposed LWE in 2005 (and LPR proposed RLWE in 2010).
  - Basis for security: worst-case to average-case reduction.
  - Most of the analysis in the literature is asymptotic.
  - Relevance to practice is qualitative, not quantitative.
  - No clean arguments for classical and quantum security.

Unpredictable new vulnerabilities

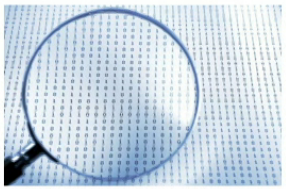
"As is the norm, an unexpected problem occurred today."


message = 001101
key = 101101
ciphertext = 100000

Strong desire to implement quantum technology



Designing new materials, drugs, etc.



Optimizing

Sensing and measuring

Secure communication

What else???

evolution

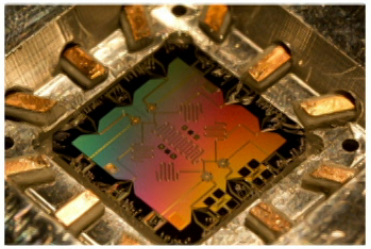
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

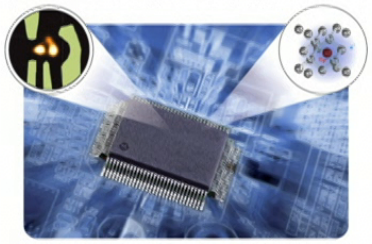
One serious problem for public-key cryptography

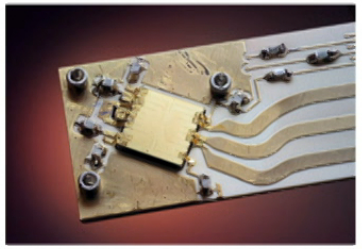
Algorithms for Quantum Computation: Discrete Logarithms and Factoring

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

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

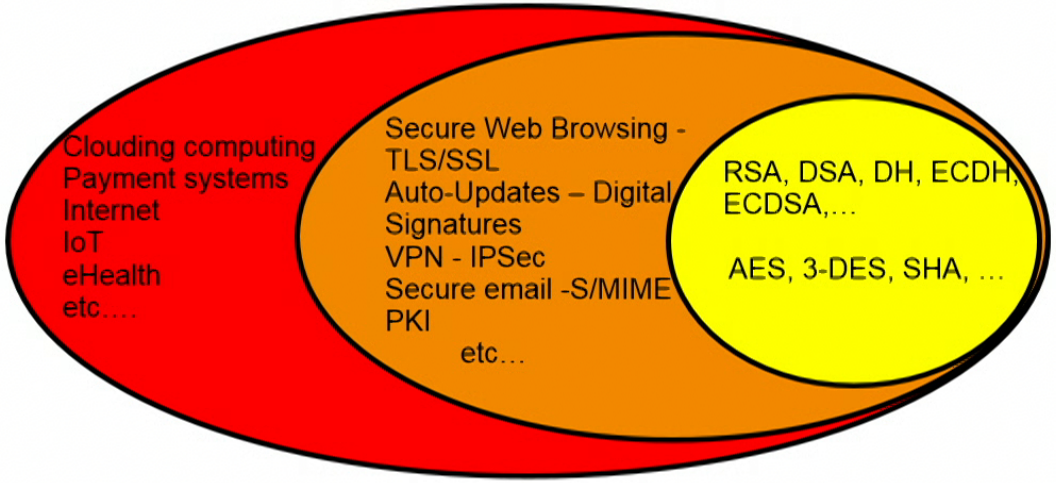
evolution

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

What will be affected?

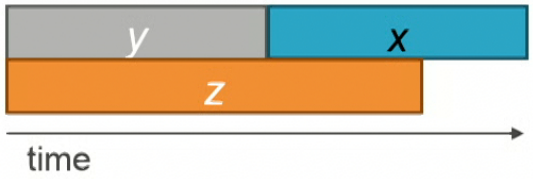


Do we need to worry *now*?

Depends on:

- X = *security shelf-life*
- Y = *migration time*
- Z = *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

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

REVIEW

Superconducting Circuits for Quantum Information: An Outlook

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

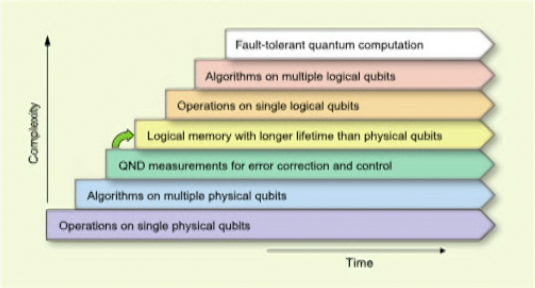


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third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

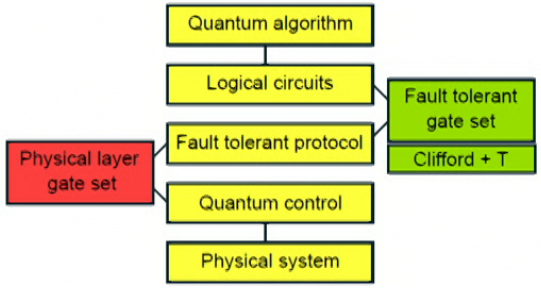
evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

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.

How large of a quantum computer is needed?



Institute for Quantum Computing » Events » 2015 » June »

Quantum Programming and Circuits Workshop

Monday, June 8, 2015 (all day) to Thursday, June 11, 2015 (all day)

The workshop aims at bringing together researchers from quantum computing and classical programming languages. Open questions that we anticipate this group to tackle include new methods for circuit synthesis and optimization, compiler optimizations and rewriting, embedded languages versus non-embedded languages, implementations of type systems and error reporting for quantum languages, techniques for verifying the correctness of quantum programs, and new techniques for compiling efficient circuits and protocols for fault-tolerant questions and their 2D layout.

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"

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

+

quantum cryptography

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Terminology

“Quantum-safe”

=

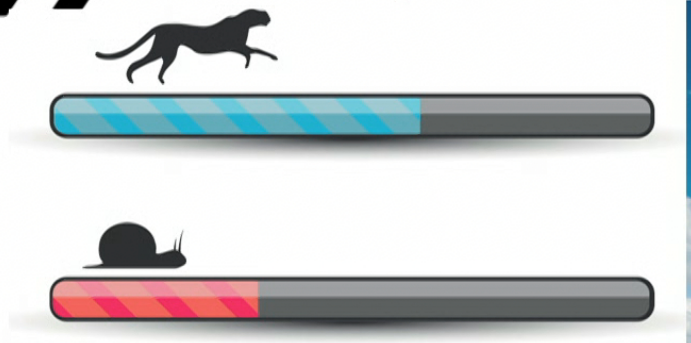
“safe in the era with large-scale quantum computers”

=

conventional “post-quantum”/ “quantum-resistant” cryptography

+ quantum cryptography

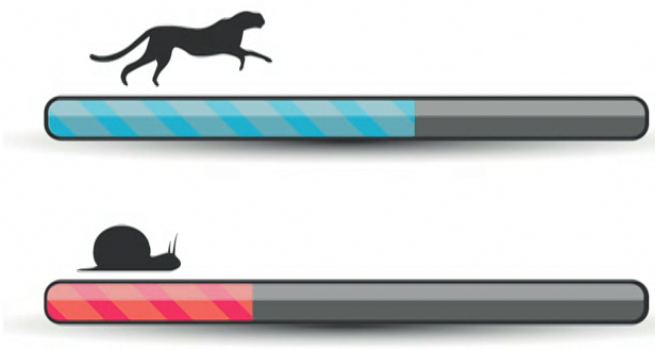
Price of procrastination?



evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

What is 'y'? How long to quantum proof?



evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Security is a choice

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

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

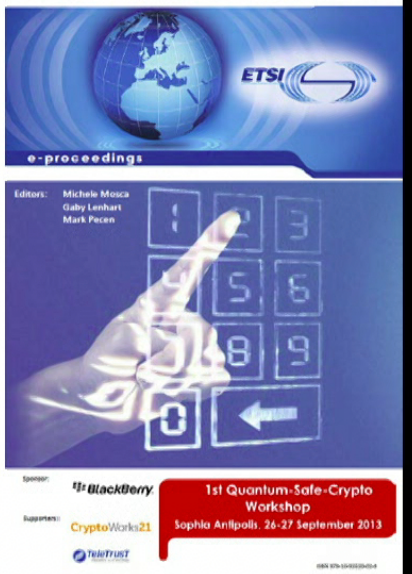
ETSI White Paper No. 8

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, hosted by SK Telecom
5-7 October, 2015, Seoul, Korea

evolution

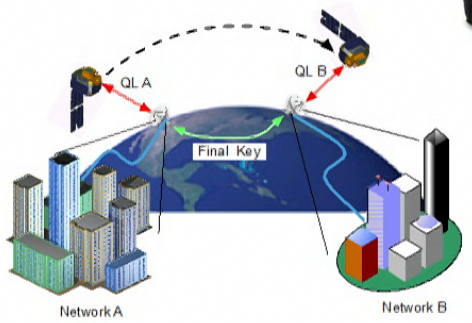
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

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”.

evolution

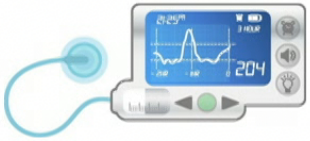
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

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.**

Don’t forget: A lot more is at stake now than we ever imagined



evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

The choice is ours

Embrace quantum technologies that will help humanity
and
live in a cyber-enhanced world designed to be safe in the quantum era

evolution

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 your 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.

- Leverage existing risk mitigation policies, procedures, and processes.
- Manage community and technical challenges to deploying quantum-safe cryptography.

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

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.

evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing