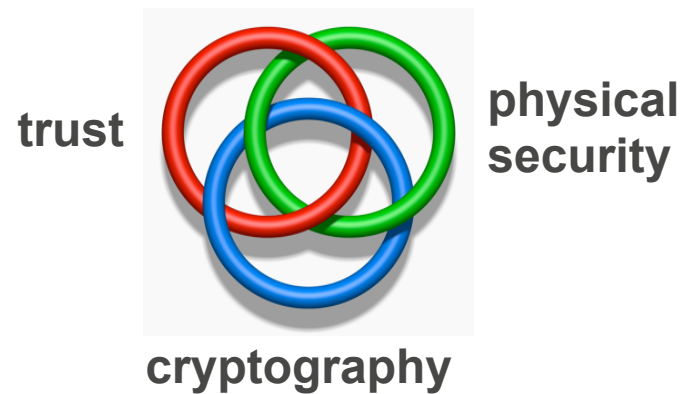


Cryptography is a foundational pillar of the global information security infrastructure

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

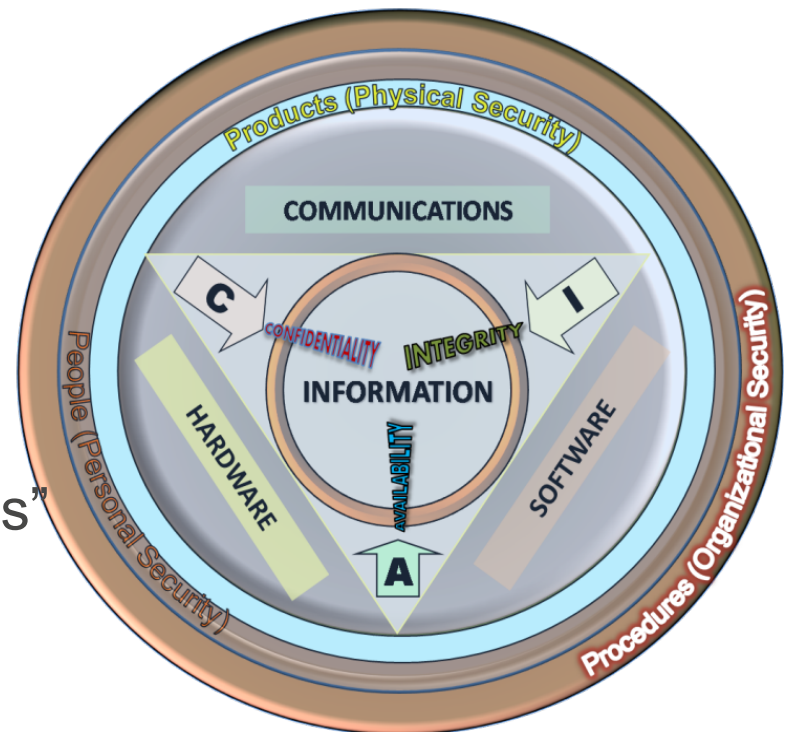
e.g. Do you update your software and anti-virus daily? Why do you trust the source?



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”



CC-BY-SA 2009 John M. Kennedy T.
<http://en.wikipedia.org/wiki/File:CIAJMK1209.png>

The problem

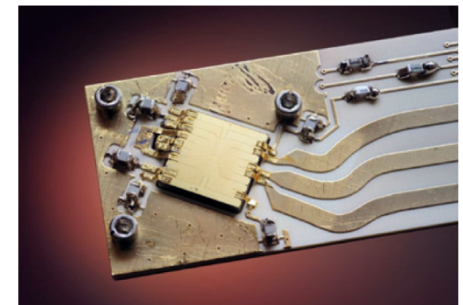
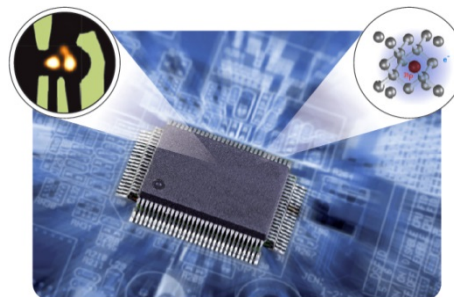
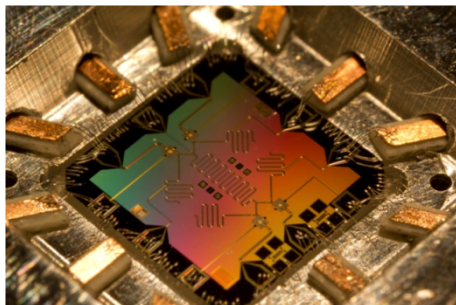


One serious problem for public-key cryptography

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





...on top of ever-present risk of unexpected advances in classical algorithms

e.g.

A quasi-polynomial algorithm for discrete logarithm
in finite fields of small characteristic

Improvements over FFS in small to medium characteristic

Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé

Cryptology ePrint Archive: Report 2013/400

Date: received 18 Jun 2013



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

How soon do we need to worry?

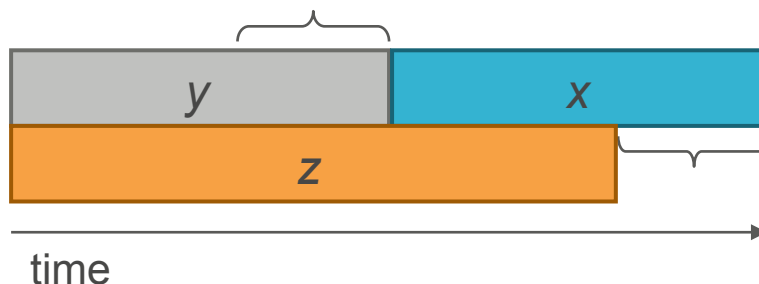
Depends on:

- 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 do we do here??



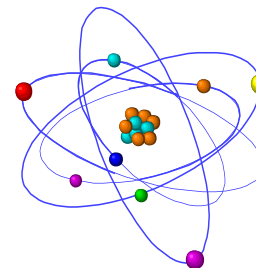
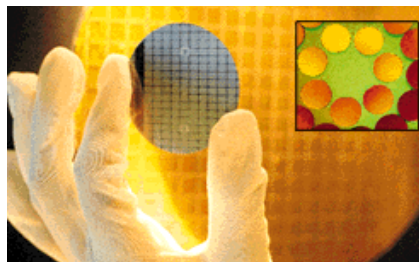
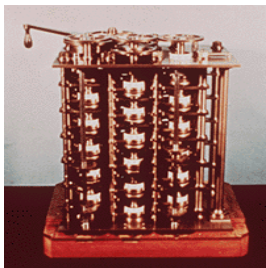


WHAT'S A QUANTUM COMPUTER??



Physics and Computation

- Information is physical...
 - Information is stored in a physical medium and manipulated by physical processes.
 - A realistic model of computation must be cast in a realistic physical framework.
 - The “classical” paradigm for physics usually provides a good approximation to the laws of physics, but not always.



Why are quantum computers apparently more powerful?

$$\begin{aligned} & \text{Three ovals with black dots and blue dots on top} \rightarrow \text{Three ovals with black dots and pink dots on top} \\ & = 0.112 \text{ (state 1)} - 0.123 \text{ (state 2)} \\ & - 0.325 \text{ (state 3)} + 0.215 \text{ (state 4)} \\ & + 0.270 \text{ (state 5)} - 0.173 \text{ (state 6)} \\ & - 0.017 \text{ (state 7)} - 0.847 \text{ (state 8)} \end{aligned}$$



- Classically simulating n quantum bits seems to require keeping track of 2^n quantum amplitudes.

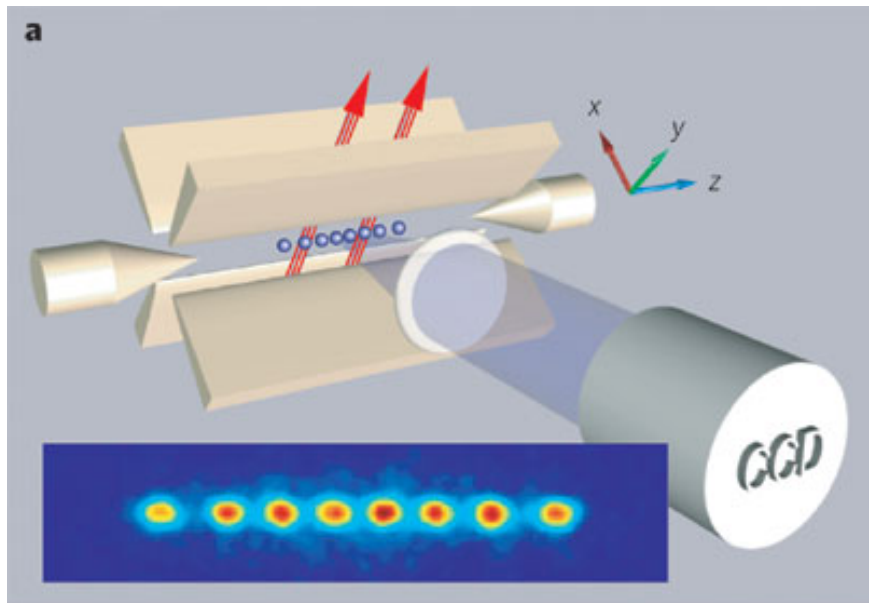
n	2^n
10	$2^{10} \approx 1\,000$
20	$2^{20} \approx 1\,000\,000$
30	$2^{30} \approx 1\,000\,000\,000 \approx \text{GB}$
40	$2^{40} \approx 1\,000\,000\,000\,000 \approx \text{TB}$
50	$2^{50} \approx 1\,000\,000\,000\,000\,000 \approx \text{PB}$

- This challenges the Strong Church-Turing thesis:
 - A probabilistic (classical) Turing machine can efficiently simulate any realistic model of computing.

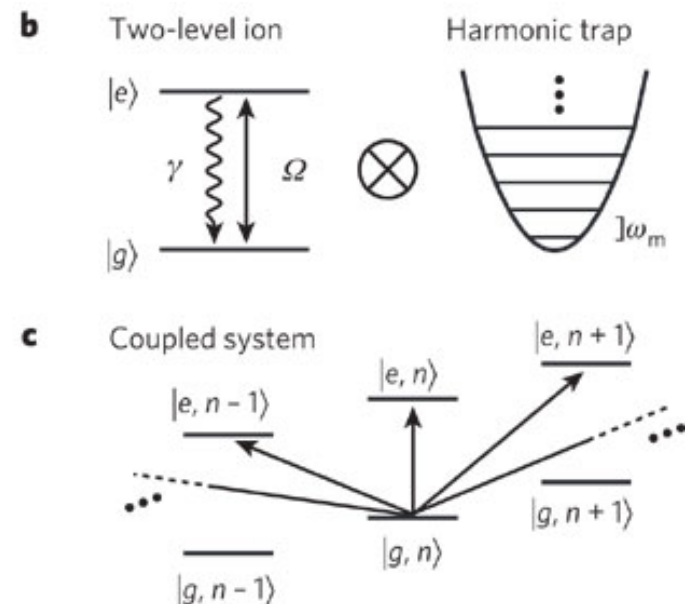


What might quantum computers look like?

■ Trapped ions?

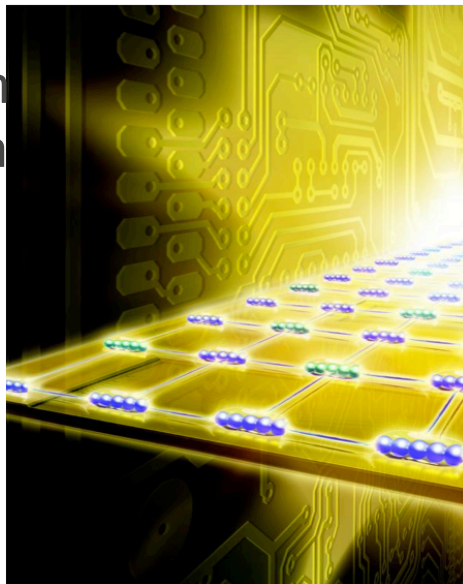


Blatt and Wineland. *Nature* **453**, 1008-1015 (2008).



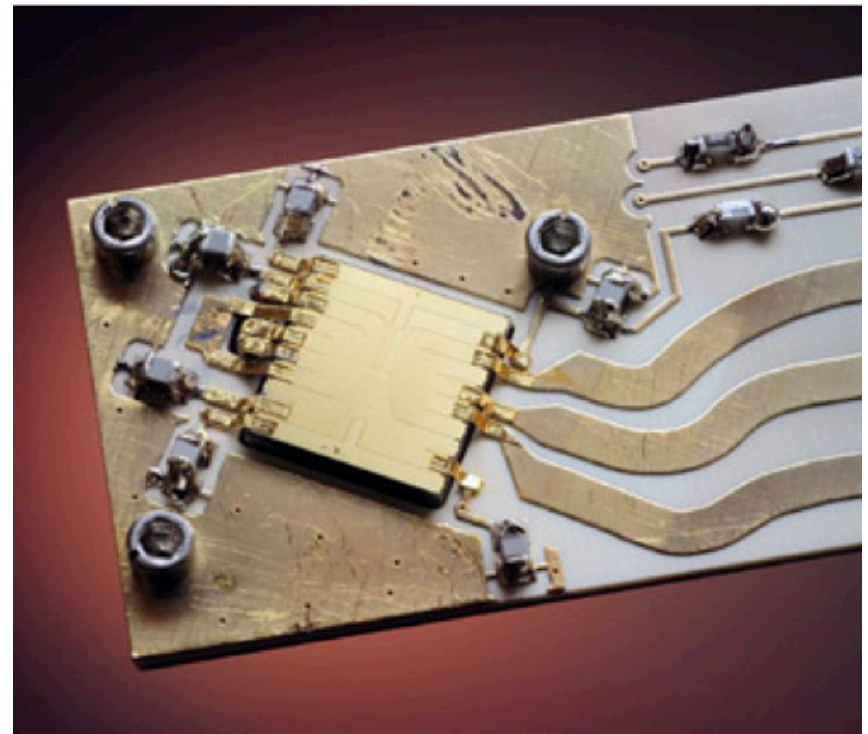


“This picture illustrates our vision of a future quantum computer. Strings of ions are held as separate strings above an ‘ion trap chip’. Through the antennae-effect, quantum information can be exchanged between neighbouring ion strings.”



© Harald Ritsch

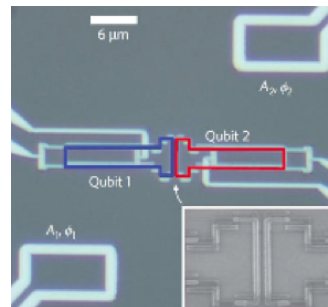
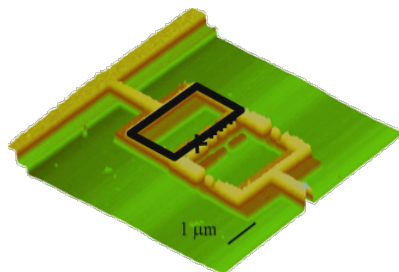
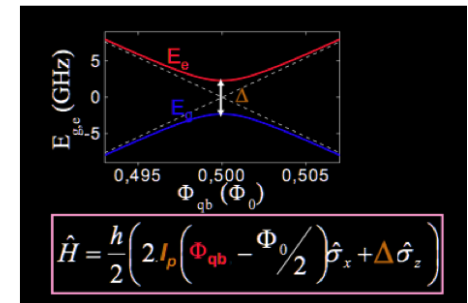
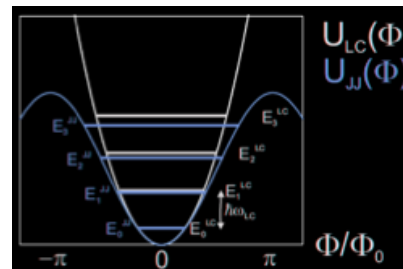
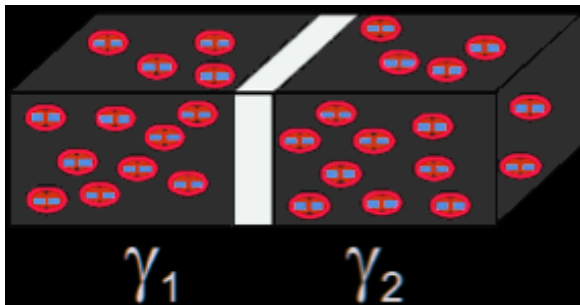
NIST’s gold ion trap on an aluminum-nitride backing

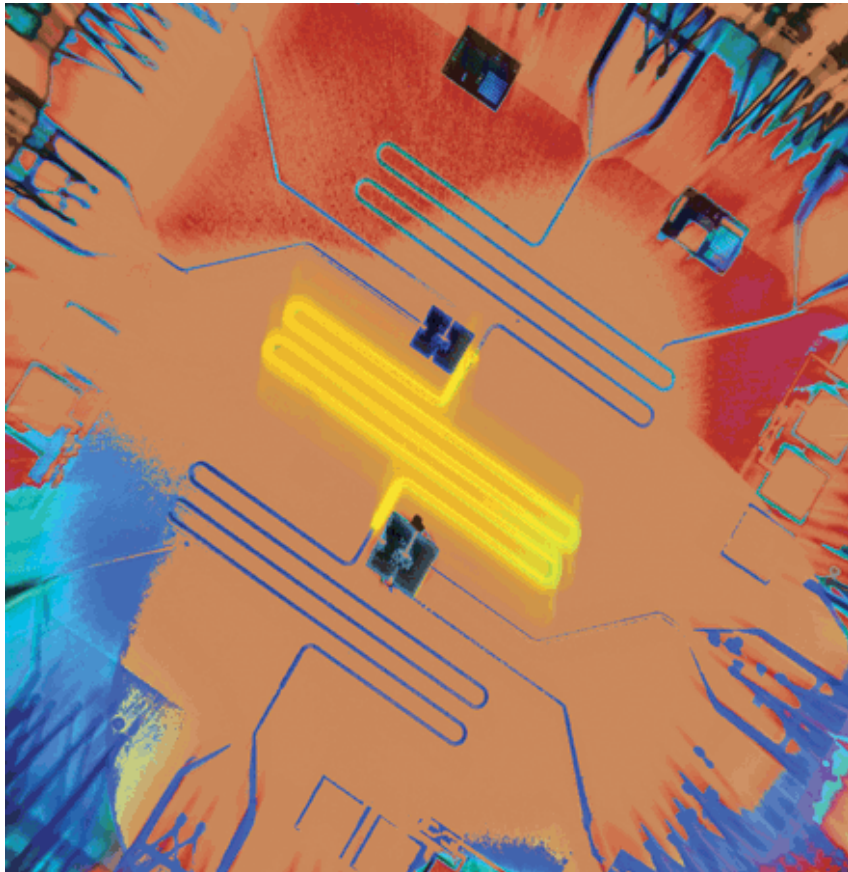


Y. Colombe/NIST

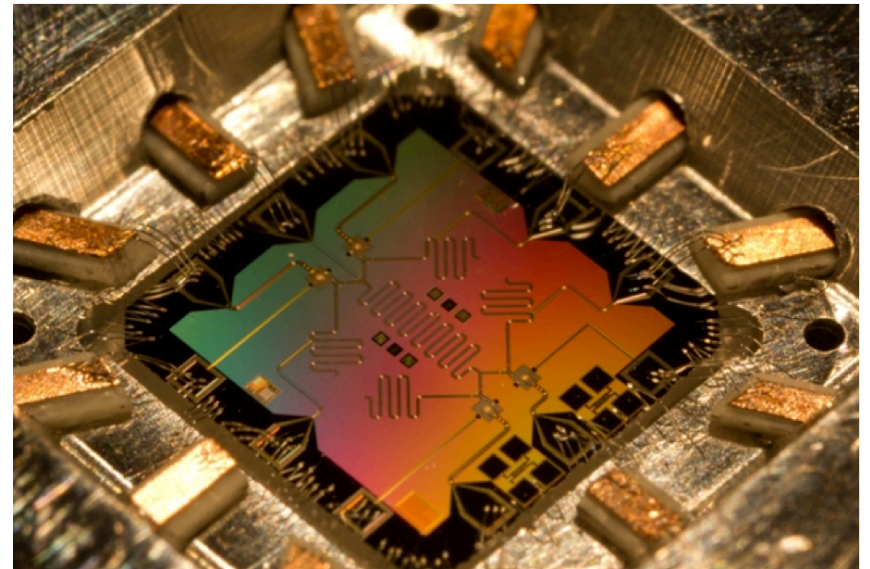
Superconducting qubits?

- Nanoelectronic circuits with linear elements and Josephson junction (non-linear inductor)





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



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



There are many other proposals,
and new ones still to be invented.

PRESSMEDDELANDE
Press release

9 October 2012

The Nobel Prize in Physics 2012

The Royal Swedish Academy of Sciences has decided to award the Nobel Prize in Physics for 2012 to

Serge Haroche

Collège de France and
Ecole Normale Supérieure, Paris, France

and

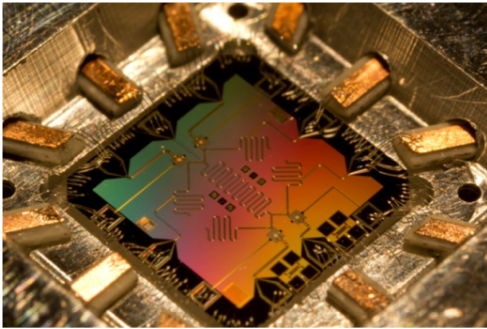
David J. Wineland

National Institute of Standards and Technology (NIST) and
University of Colorado Boulder, CO, USA

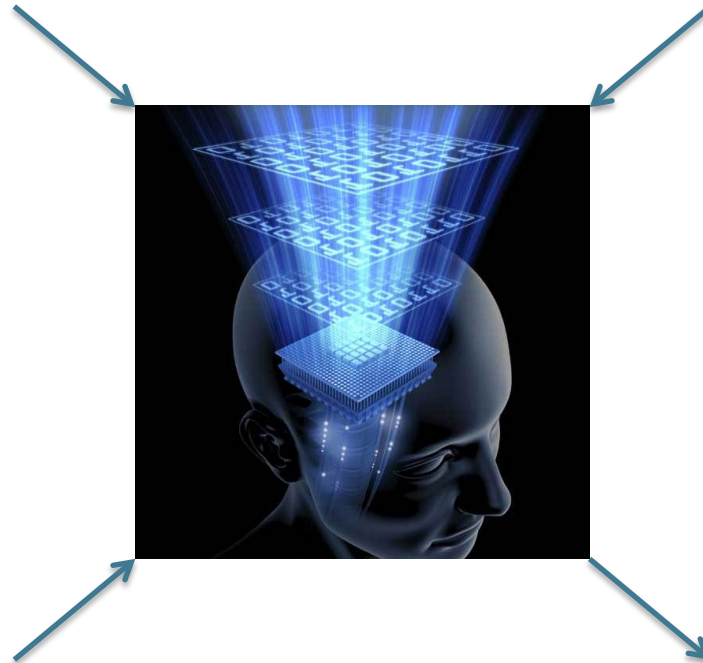
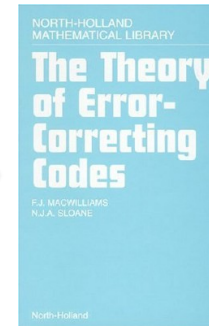
“for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems”.

Particle control in a quantum world

“Threshold theorem”

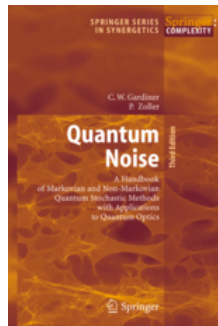


Architecture description



Threshold “ ϵ ”

If the error rates of the basic operations of the device are below ϵ ,
then we can efficiently scale quantum computations.



Error model

VOLUME 55, NUMBER 5, SEP./OCT. 2011



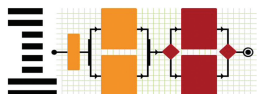
Journal of Research and Development

Including IBM Systems Journal

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.



Frontiers of Information Technology

©Copyright 2011 by International Business Machines Corporation. Copying in printed form for private use is permitted without payment of royalty provided that (1) each reproduction is done without alteration and (2) the Journal reference and IBM copyright notice are included on the first page. The title and abstract, but no other portions, of this paper may be copied by any means or distributed royalty free without further permission by computer-based and other information-service systems. Permission to republish any other portion of this paper must be obtained from the Editor.

0018-8646/11/\$5.00 © 2011 IBM



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.

©Copyright 2011 by International Business Machines Corporation. Copying in printed form for private use is permitted without payment of royalty provided that (1) each reproduction is done without alteration and (2) the Journal reference and IBM copyright notice are included on the first page. The title and abstract, but no other portions, of this paper may be copied by any means or distributed royalty free without further permission by computer-based and other information-service systems. Permission to republish any other portion of this paper must be obtained from the Editor.

0018-8646/11/\$5.00 © 2011 IBM

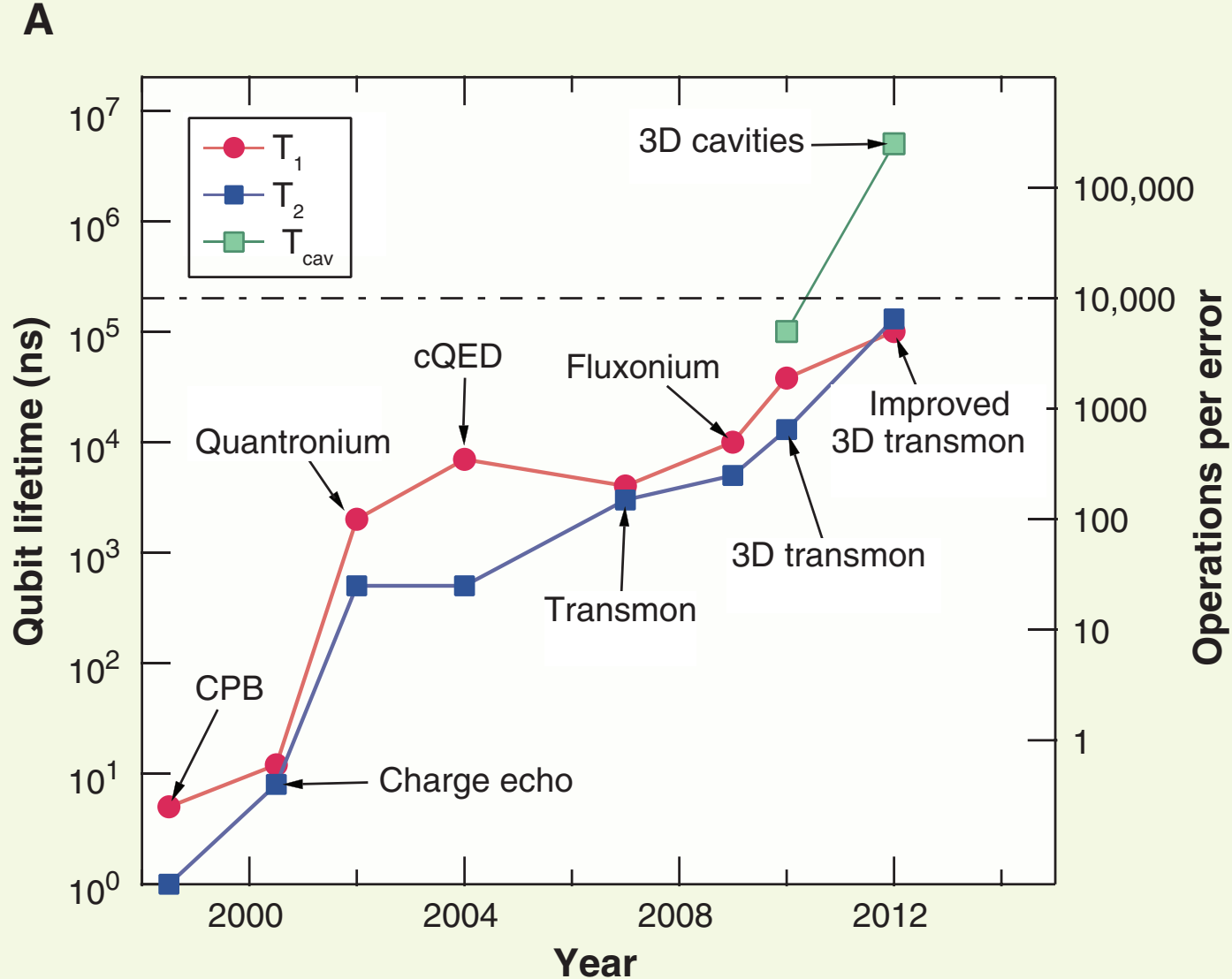
Recent progress in superconducting qubits

REVIEW

SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

Requirement for scalability	Desired capability margins	Estimated current capability	Demonstrated successful performance
QI operation			
Reset qubit	10^2 to 10^4	50	Fidelity ≥ 0.995 (17)
Rabi flop	10^2 to 10^4	1000	Fidelity ≥ 0.99 (69, 70)
Swap to bus	10^2 to 10^4	100	Fidelity ≥ 0.98 (71)
Readout qubit	10^2 to 10^4	1000	Fidelity ≥ 0.98 (51)
System Hamiltonian			
Stability	10^6 to 10^9	?	$\delta f/f$ in 1 day $< 2 \times 10^{-7}$ (43)
Accuracy	10^2 to 10^4	10 to 100	1 to 10% (43)
Yield	$>10^4$?	?
Complexity	10^4 to 10^7	10?	1 to 10 qubits (61)



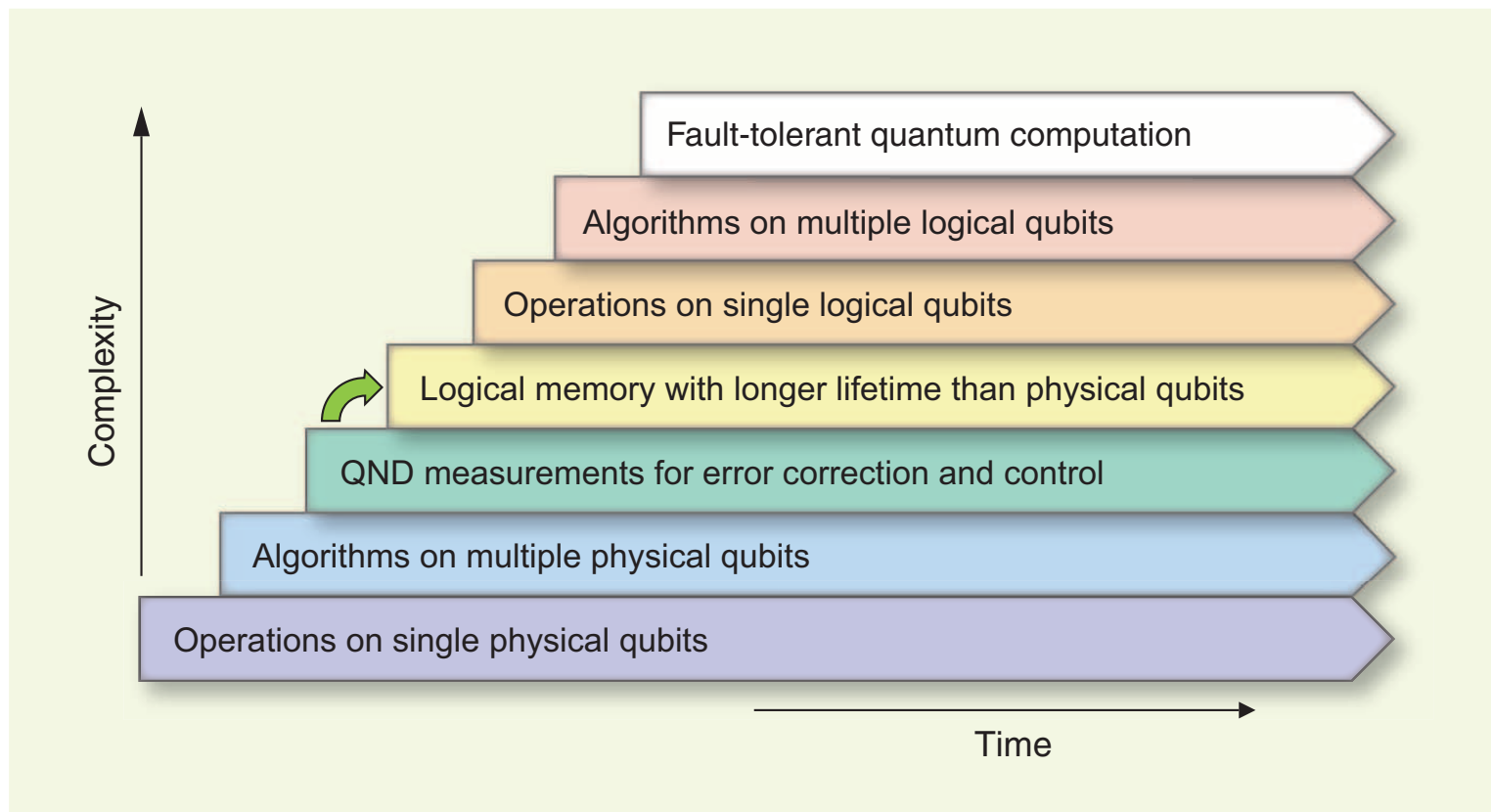


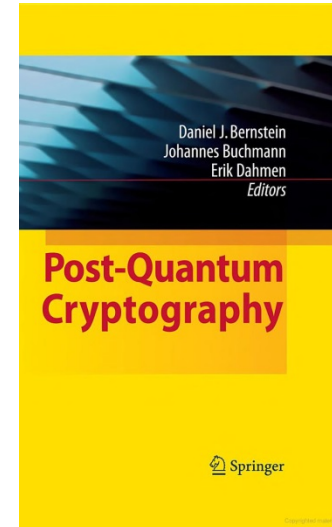
Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third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

How long to re-tool the cryptographic infrastructure?

Cryptographers are studying possible quantum-safe codes.

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

How easy is it to change from one cryptographic algorithm to a quantum-secure one? Are the standards and practices ready?



Sept. 18th - 23rd 2011,
Dagstuhl Seminar 11381
Sept. 8th - 13th 2013,
Dagstuhl Seminar 13371
TBD 2015



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

CryptoWorks21

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

Apply now!



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

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



Overview of options

Quantum-safe authentication

- Trap-door predicate based public-key signatures
- Hash-function based public-key signatures
- Symmetric-key authentication

Quantum-safe key establishment

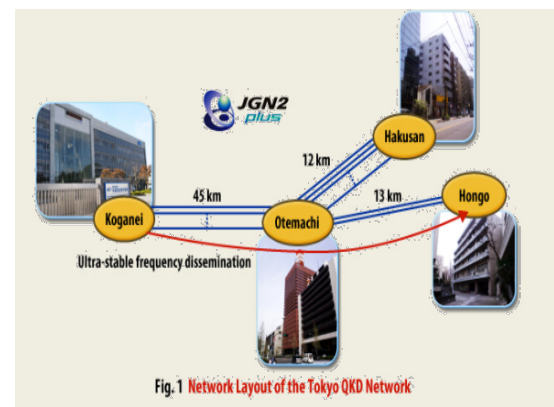
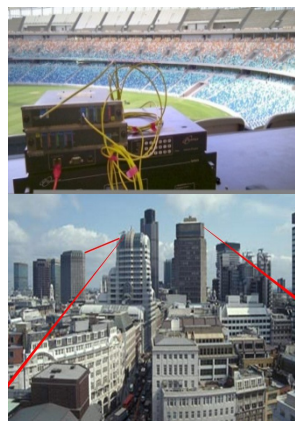
- “Alternative” public-key-encryption based key establishment
 - Lattices
 - Codes
 - Multi-variate functions
 - Other
- Quantum key establishment

Some comments about QKD

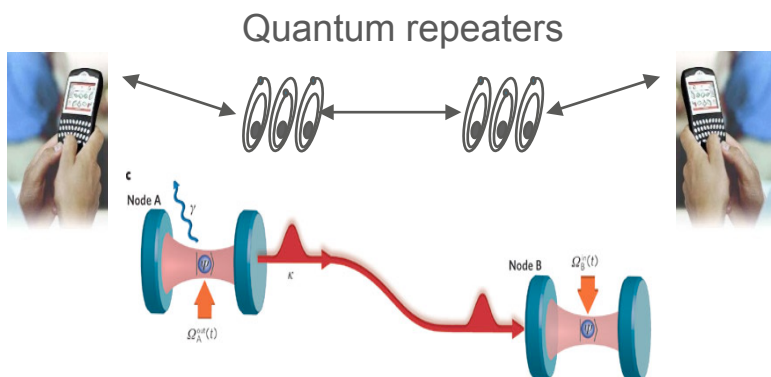
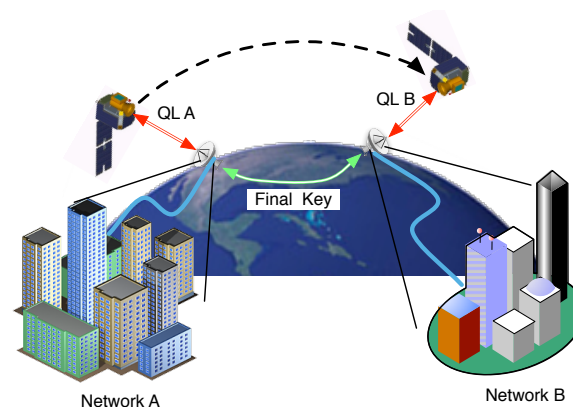
Quantum communication can provide “information theoretically” secure key establishment through an untrusted (quantum) authenticated channel.



Canary Islands:
Longest Free Space distance for QKD



- New technologies will achieve reliable quantum communication on global distances, well beyond the current range of about 100 km
 - Quantum repeaters, quantum teleportation, and satellites can be used someday to span the globe



Reviews on Quantum Repeaters: Sangouard et al, Rev. Mod. Phys. 83, 33 (2011); Kimble, NATURE, 453 (2008).

- A quantum satellite in LEO can interconnect ground networks located anywhere on Earth.
 - Active research in Canada (QEYSSAT), USA, Europe (Space-QUEST), Japan, China, Singapore.

- 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





Complexity assumptions for long-term confidentiality

Signature/

key-establishment/

encryption combination

- Symmetric key authentication + QKD+OTP
- Hash-based signatures + QKD +OTP
- Hash-based signatures + QKD +AES
- Trapdoor based signatures + QKD+AES
- Trapdoor based signatures + trapdoor based key establishment +AES

Strongest computational assumption

- No computational assumptions.
- Short-term security of OWF
- Long-term security of OWF
- Short-term security of trapdoor predicate + long-term security of OWF
- Long-term security of trapdoor predicate

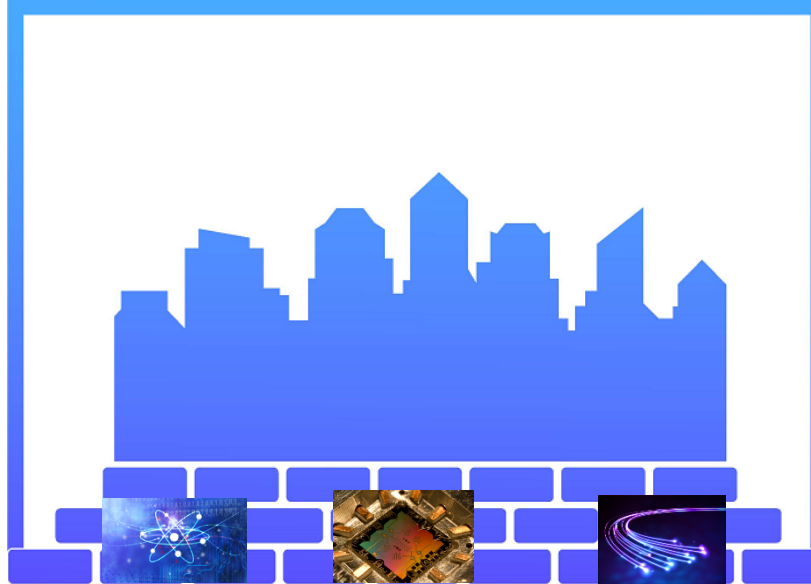
Overcoming obstacles to quantum-proofing

Challenges

- Performance
- Battle-testing:
 - Implementation errors
 - Protocol errors
 - Side-channel attacks
 - etc
- Availability
- Resistance to replacing 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.



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***.



- Get quantum-safe options on vendor roadmaps
 - Routinely ask about vulnerability of systems to quantum attacks
 - Include quantum-safe options in RFPs
 - 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

Thank you!

- Feedback welcome: mmosca@iqc.ca

Our supporters...

Canada

Ontario



Canadian Institute for
Advanced Research

CryptoWorks21



Canada Foundation
for Innovation

Fondation canadienne
pour l'innovation

