

Title: Introduction to Quantum Information Processing

Date: Jul 20, 2011 08:30 AM

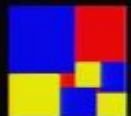
URL: <http://pirsa.org/11070091>

Abstract: <div id="Cleaner">Information processing is a physical process, and thus the powers and limitations of an information processing device depend on the laws of physics. The “classical” framework for physics has long been replaced by quantum physics. Over the past century we have moved from observing quantum phenomena to controlling quantum phenomena. Remarkable progress has been made in recent years. Very importantly, the quantum features of nature lead to qualitatively different and apparently more powerful models of computation and communication. Quantum computers can efficiently solve problems that were previously believed to be intractable. Quantum information also enables communication and cryptographic tasks that would otherwise not be possible. I will introduce quantum information processing and summarize the state of the art.</div></span>

*Michele Mosca*  
*Canada Research Chair in Quantum Computation*

20 July 2011

# Women in Physics Canada



COMBINATORICS  
& OPTIMIZATION

UNIVERSITY OF  
**WATERLOO**

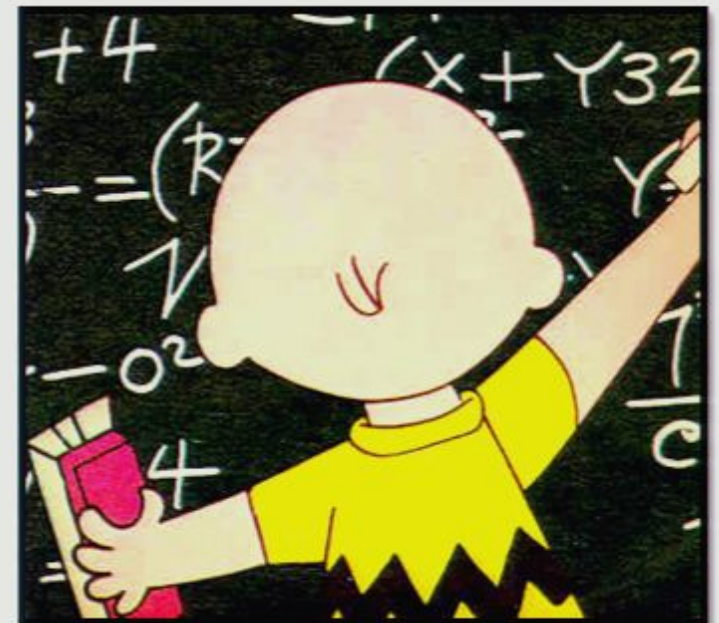
**IQC**

Institute for  
Quantum  
Computing



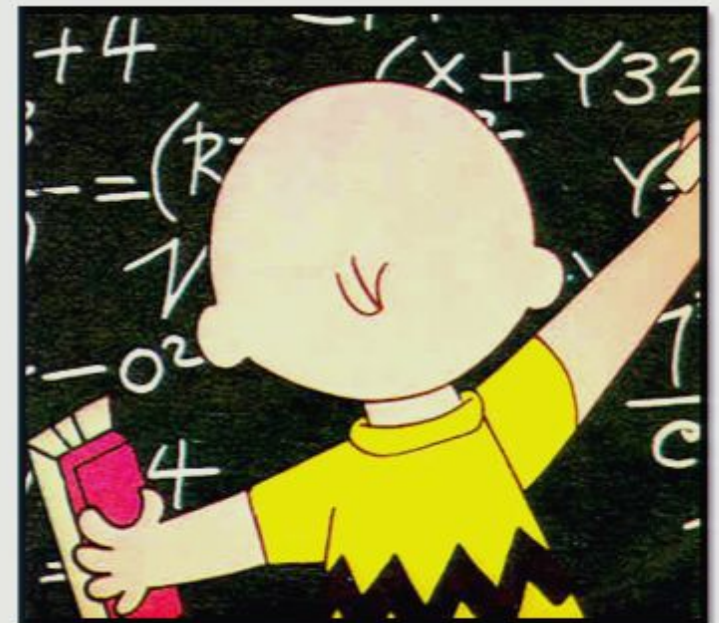
# How I got into quantum information

Started my studies in the mathematics behind modern cryptography



# How I got into quantum information

Started my studies in the mathematics behind modern cryptography



# “Computationally secure” cryptography

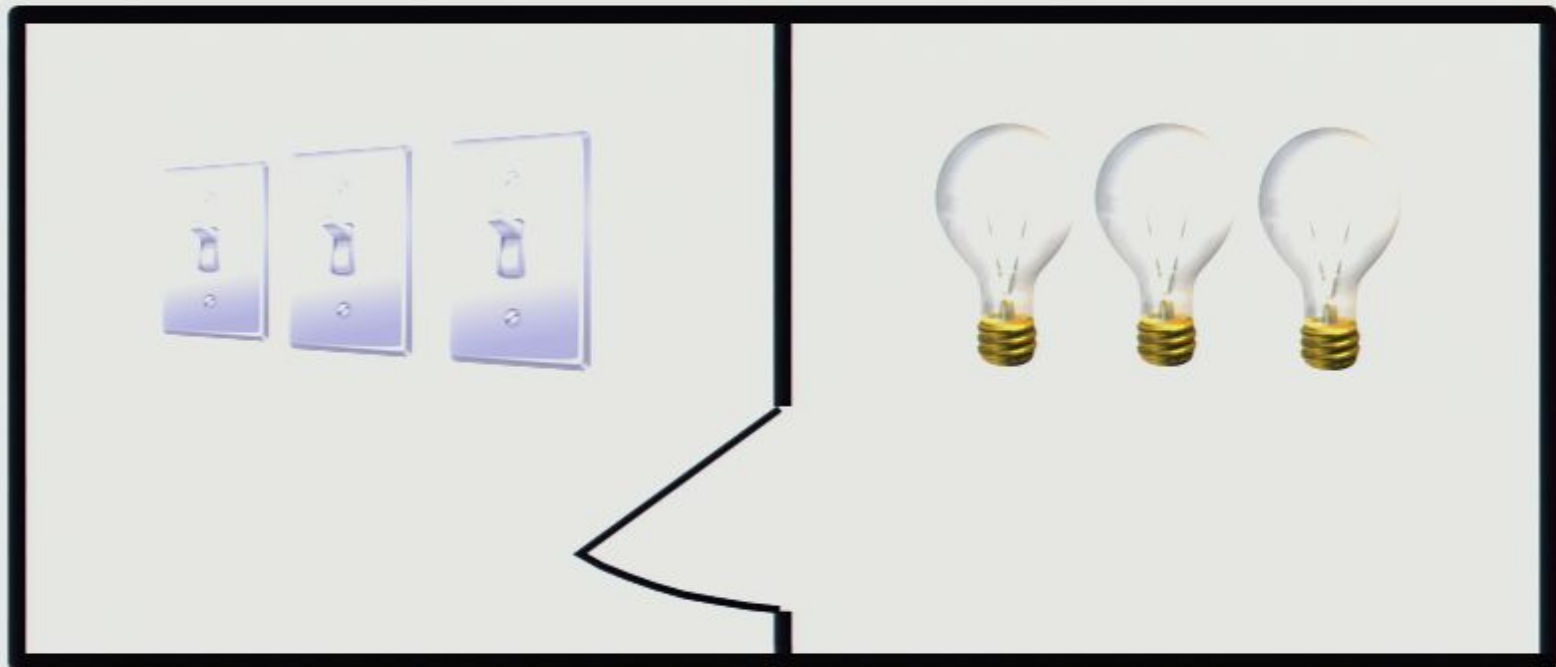


Most of modern cryptography relies on the impracticality of solving a hard mathematical problem.

I learned that most of these assumptions are probably wrong.

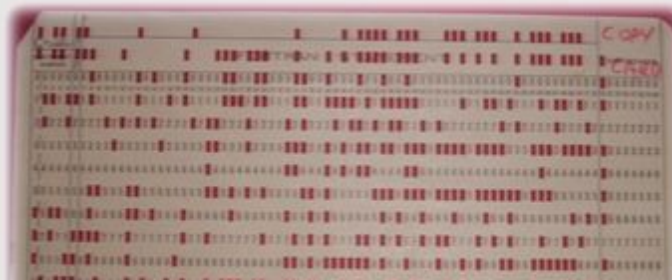
# Information is physical

**Problem:** Consider a setup with two rooms. In one room, there are three switches, each of which can be either on or off. In the next room, there are three light bulbs, each one corresponding to one of the switches, in a one-to-one manner. Your task is to determine which switch corresponds to which bulb. However, you may only enter the room with the bulbs once.



# Information is physical

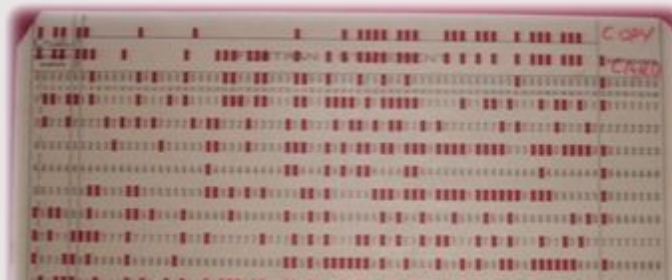
In classical computing, information is stored in *bits*. How exactly is a bit stored?



# Information is physical

In classical computing, information is stored in *bits*. How exactly is a bit stored?

We can use any two-state system. For example:

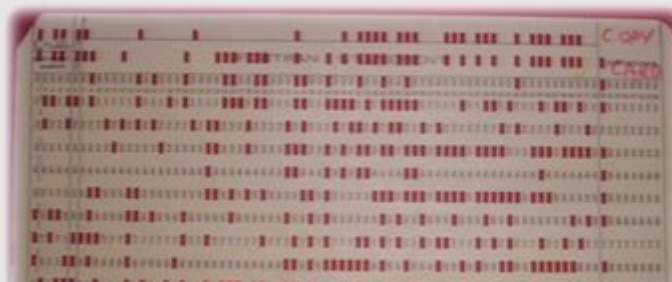


# Information is physical

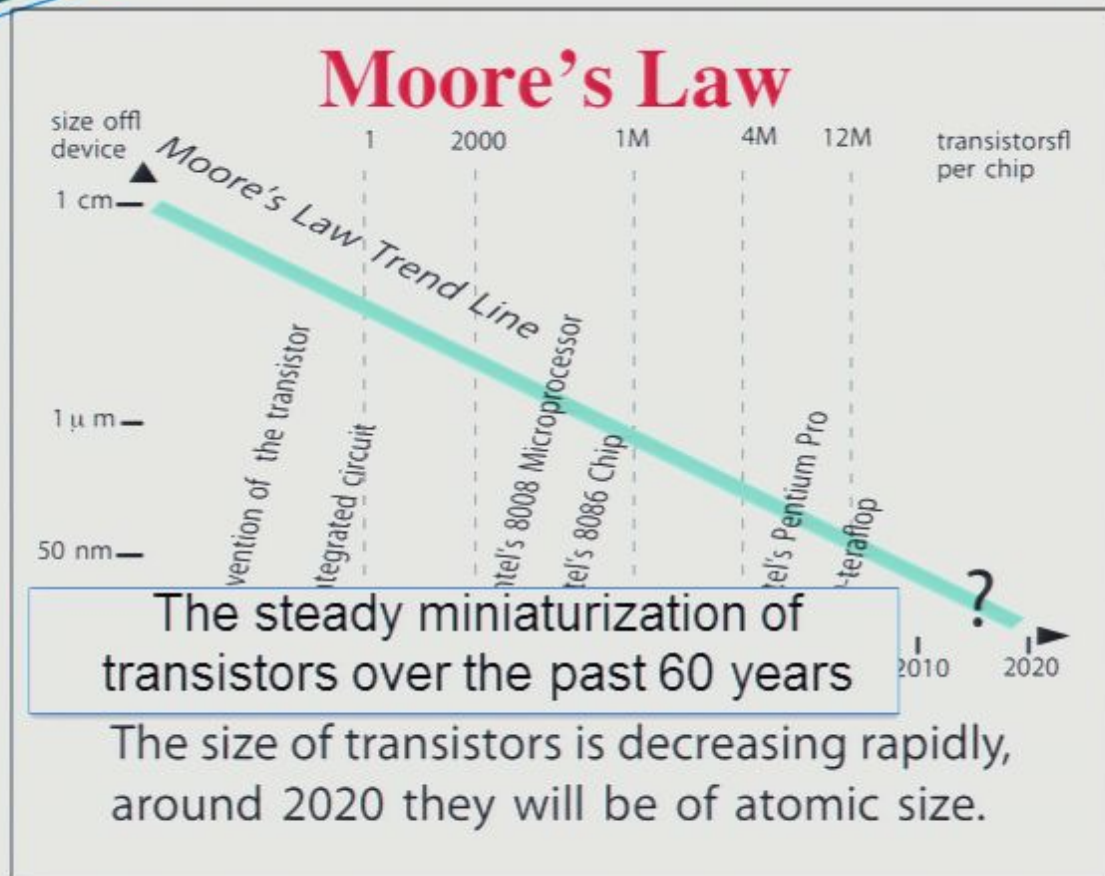
In classical computing, information is stored in *bits*. How exactly is a bit stored?

We can use any two-state system. For example:

- a wire which either has some or no electricity going through it (for example, in most RAM)
- the direction of magnetization (in a cassette tape or a floppy disk)
- a punch card has a series of spaces where there can be either a hole, or no hole
- at any location on a cd, there is either a small hole in the plastic, or not



# Toward the quantum world



## Enter Quantum Effects

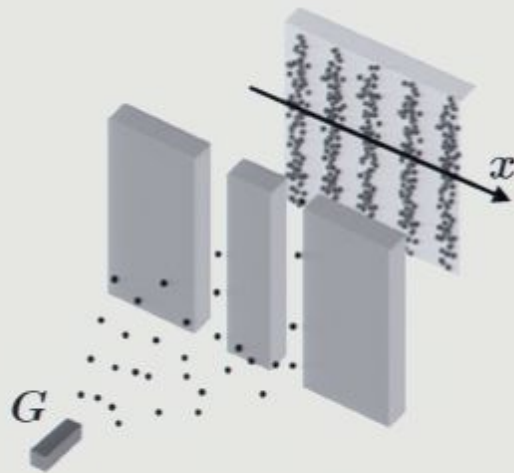
Superposition Principle

Objects can be in multiple

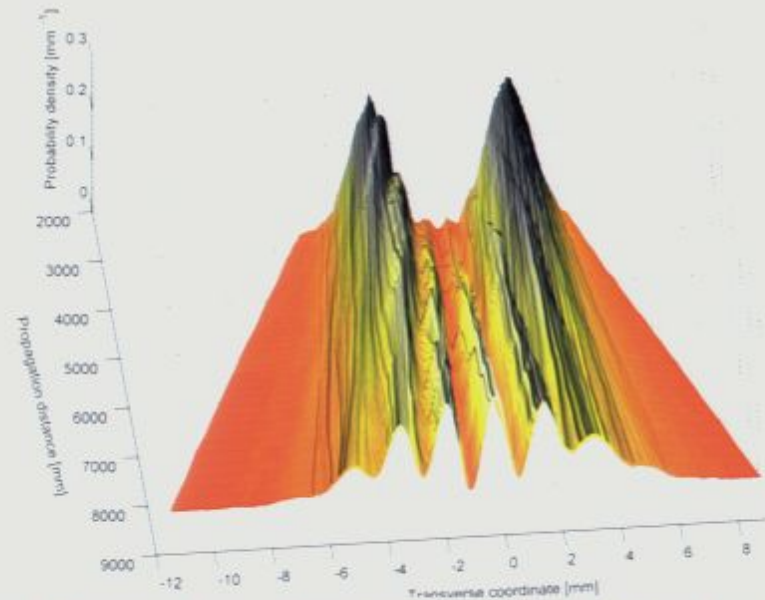
Uncertainty Principle

Merely observing a quantum

## The Uncertainty Principle: gives intrinsic eavesdropper detectability



[commons.wikimedia.org/wiki/Image:2slits.png](https://commons.wikimedia.org/wiki/Image:2slits.png)



**Fig. 4.** The trajectories from Fig. 3 plotted on top of the measured probability density distribution. Even though the trajectories were reconstructed by using only local knowledge, they reproduce the global propagation behavior of the interference pattern.



### Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer

Sacha Kocsis, *et al.*

*Science* **332**, 1170 (2011);

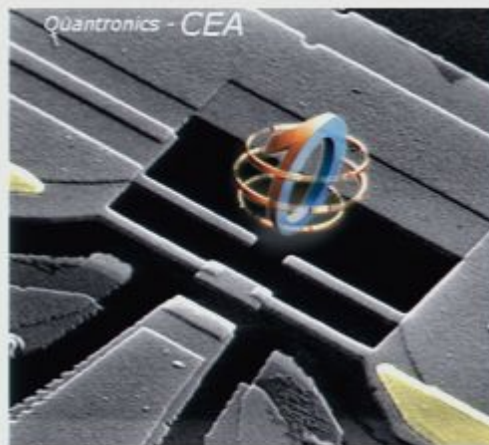
DOI: 10.1126/science.1202218

**Strong (classical) Church-Turing thesis:** a classical computer can efficiently simulate any realistic computer

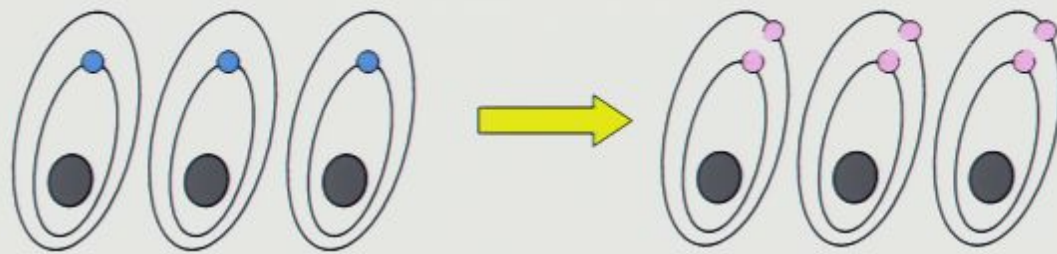


**Strong (classical) Church-Turing thesis:** a classical computer can efficiently simulate any realistic computer

Storing and manipulating information according to the laws of quantum theory, allows us to efficiently perform computations we do not believe are possible on a classical computer.



# Why are quantum computers apparently more powerful?



$$\begin{aligned} &= 0.112 \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} - 0.123 \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \\ &- 0.325 \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} + 0.215 \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \\ &+ 0.270 \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} - 0.173 \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \\ &- 0.017 \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} \begin{array}{c} \text{blue dot} \\ \text{oval} \end{array} - 0.847 \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \begin{array}{c} \text{pink dot} \\ \text{oval} \end{array} \end{aligned}$$

# Need to reassess computational security

	Classically (best known heuristic algorithms)	Quantumly
Factoring n-digit number	$e^{O(n^{1/3} \log^{2/3} n)}$	$O(n)$ multiplications
Discrete log in GF(q), $q \approx 2^n$	$e^{O(n^{1/3} \log^{2/3} n)}$	$O(n)$ multiplications
Discrete log in EC(q), $q \approx 2^n$	$e^{O(n)}$	$O(n)$ additions

# How soon do we need to worry?



# How soon do we need to worry?

Depends on:

- How long do you need encryption to be secure? ( $x$  years)

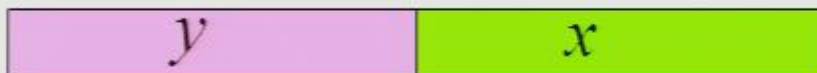
$x$



# 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? ( $y$  years)



# 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? ( $y$  years)
- How long will it take for a large-scale quantum computer to be built (or a new algorithm to be found, etc.)? ( $z$  years)



# 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? ( $y$  years)
- How long will it take for a large-scale quantum computer to be built (or a new algorithm to be found, etc.)? ( $z$  years)

*THEOREM 1: If  $x+y > z$  then worry.*





So how long will it take to build a large-scale quantum computer?



# So how long will it take to build a large-scale quantum computer?

A correct answer:

# So how long will it take to build a large-scale quantum computer?

A correct answer: I don't know.

# So how long will it take to build a large-scale quantum computer?

A correct answer: I don't know.

A useful answer?

THEORY

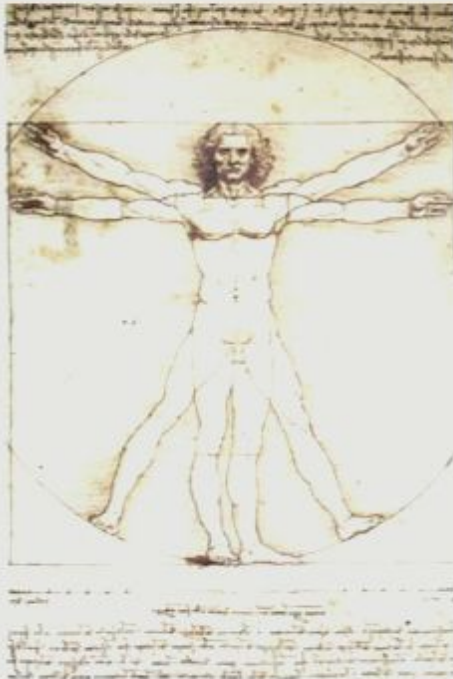


# So how long will it take to build a large-scale quantum computer?

A correct answer: I don't know.

A useful answer?

THEORY



PRACTICE



The header features a dark blue background with a pattern of glowing green binary digits (0s and 1s). A thin, curved line in shades of blue and purple arcs across the top of the slide, separating the header from the main content area.

# So how long will it take?

A useful answer:

# So how long will it take?

A useful answer:

- For reasonable architectures and error-models, there exists a constant threshold, such that components with error rates below that threshold give scalable QC

# So how long will it take?

## A useful answer:

- For reasonable architectures and error-models, there exists a constant threshold, such that components with error rates below that threshold give scalable QC
- Theorists are developing better and better methods for doing large-scale quantum computing using imperfect components

# So how long will it take?

## A useful answer:

- For reasonable architectures and error-models, there exists a constant threshold, such that components with error rates below that threshold give scalable QC
- Theorists are developing better and better methods for doing large-scale quantum computing using imperfect components
- Further developing quantum error-correcting codes, application to broader range of architectures and computing models, better understanding of thresholds and error models

# So how long will it take?

## A useful answer:

- For reasonable architectures and error-models, there exists a constant threshold, such that components with error rates below that threshold give scalable QC
- Theorists are developing better and better methods for doing large-scale quantum computing using imperfect components
- Further developing quantum error-correcting codes, application to broader range of architectures and computing models, better understanding of thresholds and error models
- We are better understanding realistic error models

# So how long will it take?

## A useful answer:

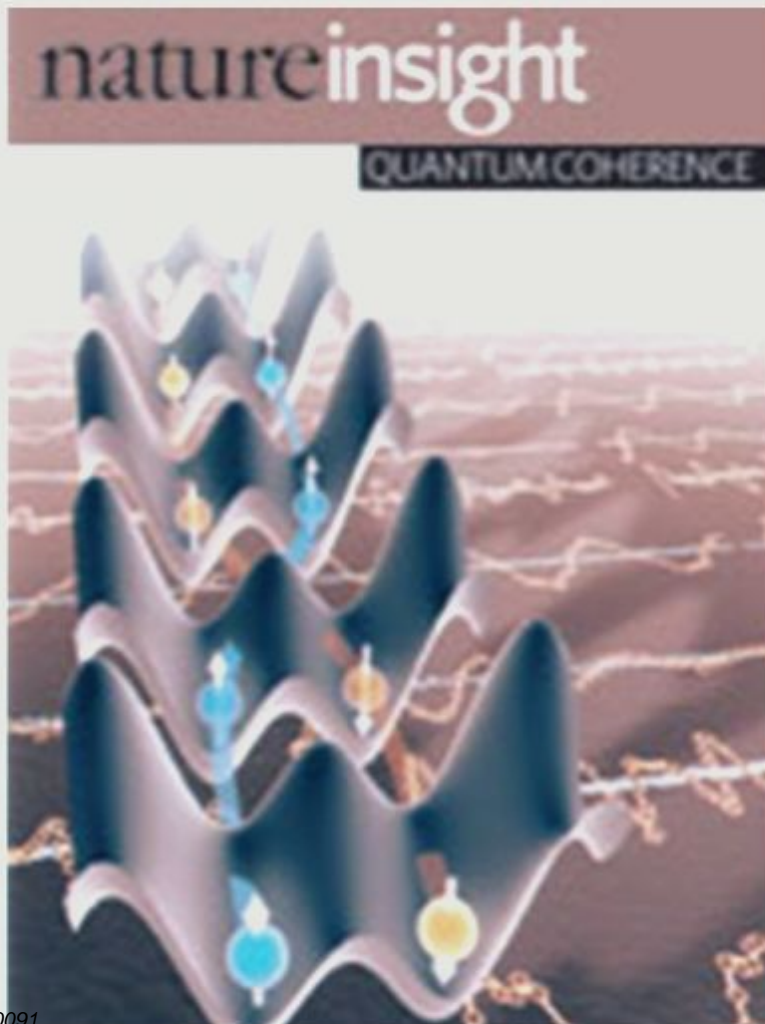
- For reasonable architectures and error-models, there exists a constant threshold, such that components with error rates below that threshold give scalable QC
- Theorists are developing better and better methods for doing large-scale quantum computing using imperfect components
- Further developing quantum error-correcting codes, application to broader range of architectures and computing models, better understanding of thresholds and error models
- We are better understanding realistic error models
- Experimentalists are gaining better control over quantum systems in a broad range of physical systems

# So how long will it take?

## A useful answer:

- For reasonable architectures and error-models, there exists a constant threshold, such that components with error rates below that threshold give scalable QC
- Theorists are developing better and better methods for doing large-scale quantum computing using imperfect components
- Further developing quantum error-correcting codes, application to broader range of architectures and computing models, better understanding of thresholds and error models
- We are better understanding realistic error models
- Experimentalists are gaining better control over quantum systems in a broad range of physical systems

Vol. 453, No. 7198 (19 June 2008) issue of Nature



**Improvements in techniques to manipulate light and matter are facilitating exciting applications of quantum mechanics.**

Scientists from diverse areas of research are now seeking to harness and exploit quantum coherence and entanglement for quantum simulations and quantum information processing.

## REVIEWS

## Quantum computers

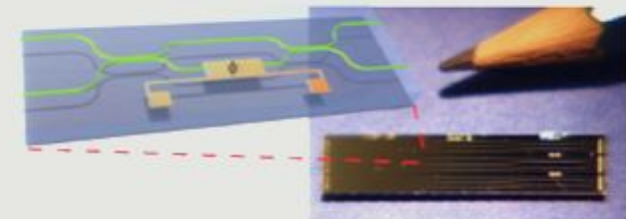
T. D. Ladd<sup>1†</sup>, F. Jelezko<sup>2</sup>, R. Laflamme<sup>3,4,5</sup>, Y. Nakamura<sup>6,7</sup>, C. Monroe<sup>8,9</sup> & J. L. O'Brien<sup>10</sup>

Over the past several decades, quantum information science has emerged to seek answers to the question: can we gain some advantage by storing, transmitting and processing information encoded in systems that exhibit unique quantum properties? Today it is understood that the answer is yes, and many research groups around the world are working towards the highly ambitious technological goal of building a quantum computer, which would dramatically improve computational power for particular tasks. A number of physical systems, spanning much of modern physics, are being developed for quantum computation. However, it remains unclear which technology, if any, will ultimately prove successful. Here we describe the latest developments for each of the leading approaches and explain the major challenges for the future.

**Table 1 | Current performance of various qubits**

Type of qubit	$T_2$	Benchmarking (%)		References
		One qubit	Two qubits	
Infrared photon	0.1 ms	0.016	1	20
Trapped ion	15 s	0.48 <sup>†</sup>	0.7*	104–106
Trapped neutral atom	3 s	5		107
Liquid molecule nuclear spins	2 s	0.01 <sup>†</sup>	0.47 <sup>†</sup>	108
$e^-$ spin in GaAs quantum dot	3 $\mu$ s	5		43, 57
$e^-$ spins bound to $^{31}\text{P}$ / $^{29}\text{Si}$	0.6 s	5		49
$^{29}\text{Si}$ nuclear spins in $^{28}\text{Si}$	25 s	5		50
NV centre in diamond	2 ms	2	5	60, 61, 65
Superconducting circuit	4 $\mu$ s	0.7 <sup>†</sup>	10*	73, 79, 81, 109

Measured  $T_2$  times are shown, except for photons where  $T_2$  is replaced by twice the hold-time (comparable to  $T_2$ ) of a telecommunication-wavelength photon in fibre. Benchmarking values show approximate error rates for single or multi-qubit gates. Values marked with asterisks are found by quantum process or state tomography, and give the departure of the fidelity from 100%. Values marked with daggers are found with randomized benchmarking<sup>90</sup>. Other values are rough experimental gate error estimates. In the case of photons, two-qubit gates fail frequently but success is heralded; error rates shown are conditional on a heralded success. NV, nitrogen vacancy.



**Figure 2 | Photonic quantum computer.** A microchip containing several silica-based waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates<sup>91</sup>. Green lines show optical waveguides; yellow components are metallic contacts. Pencil tip shown for scale.



laflamme-...





laflamme-nature08812.pdf - Adobe Acrobat Pro

File Edit View Document Comments Forms Tools Advanced Window Help

Create Combine Collaborate Secure Sign Forms Multimedia Comment

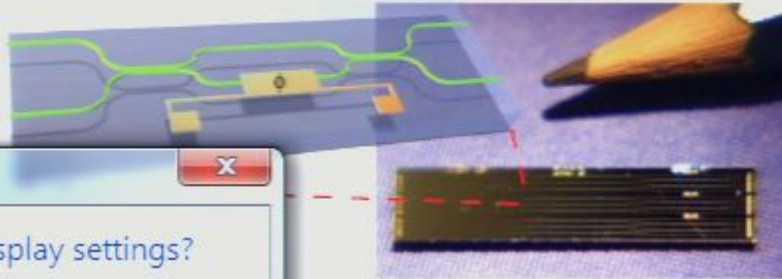
3 / 9 105% Find

and to resolve the photon number<sup>16,17</sup>. Superconducting detectors operating as sensitive thermometers can resolve the photon number, have 95% efficiency and low noise, but operate at  $\sim 100$  mK and are relatively slow. Faster (hundreds of MHz) nanostructured NbN superconducting nanowire detectors have achieved high efficiency and photon number resolution<sup>16,17</sup>.

One approach to a high-efficiency single-photon source is to multiplex the nonlinear optical sources currently used to emit pairs of photons spontaneously<sup>18</sup>. An alternative is a single quantum system in an optical cavity that emits a single photon when excited to a ground state. Robust alignment with solid-state 'artificial atoms', such as quantum dots, potentially with impurities in diamond, or with these cavity quantum electrodynamics systems provide deterministic photon-photon interactions.

Regardless of the approach used, the challenge of nonlinearities, photon loss remains.

optical spin-dependent forces that do not require individual optical addressing of the ions, nor the preparation of the ionic motion into a



Microsoft Windows

Do you want to keep these display settings?

No projector was detected.

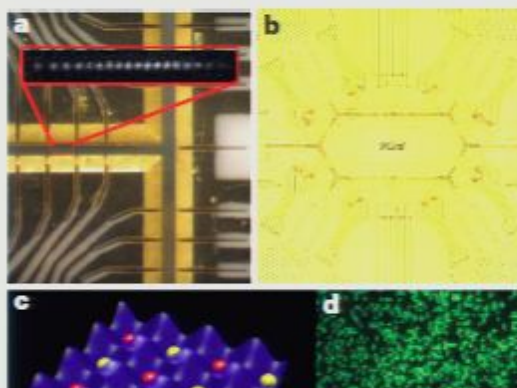
Keep changes Revert

Reverting to previous display settings in 7 seconds.

47

## REVIEWS

NATURE|Vol 464|4 March 2010



optical lattices for quantum computing are the controlled initialization, interaction and measurement of the atomic qubits. However, there has been much progress on all of these fronts in recent years.

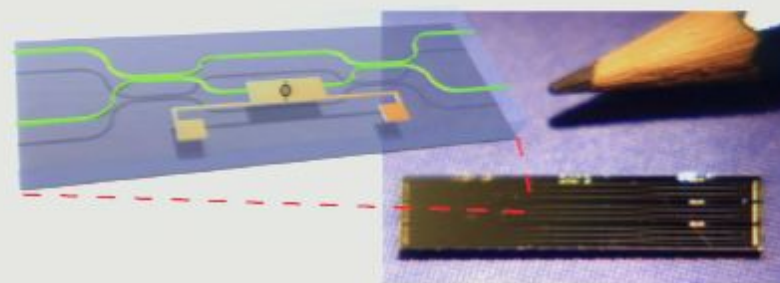
Optical lattices are typically loaded with  $10^3$ – $10^6$  identical atoms, usually with non-uniform packing of lattice sites for thermal atoms. However, when a Bose condensate is loaded in an optical lattice, the competition between intrasite tunnelling and the on-site interaction between multiple atoms can result in a Mott-insulator transition where approximately the same number of atoms (for example, one) reside in every lattice site<sup>14</sup>. The interaction between atomic qubits in optical lattices can be realized in several ways. Adjacent atoms can be brought together depending on their internal qubit

and to resolve the photon number<sup>16,17</sup>. Superconducting detectors operating as sensitive thermometers can resolve the photon number, have 95% efficiency and low noise, but operate at  $\sim 100$  mK and are relatively slow. Faster (hundreds of MHz) nanostructured NbN superconducting nanowire detectors have achieved high efficiency and photon number resolution<sup>16,17</sup>.

One approach to a high-efficiency single-photon source is to multiplex the nonlinear optical sources currently used to emit pairs of photons spontaneously<sup>18</sup>. An alternative is a single quantum system in an optical cavity that emits a single photon on transition from an excited to a ground state. Robust alignment of the cavity can be achieved with solid-state 'artificial atoms', such as quantum dots<sup>18,19,21,22</sup> and potentially with impurities in diamond<sup>23</sup>, which we discuss below. As these cavity quantum electrodynamics systems improve, they could provide deterministic photon-photon nonlinearities<sup>24</sup>.

Regardless of the approach used for photon sources, detectors and nonlinearities, photon loss remains a significant challenge, and

optical spin-dependent forces that do not require individual optical addressing of the ions, nor the preparation of the ionic motion into a



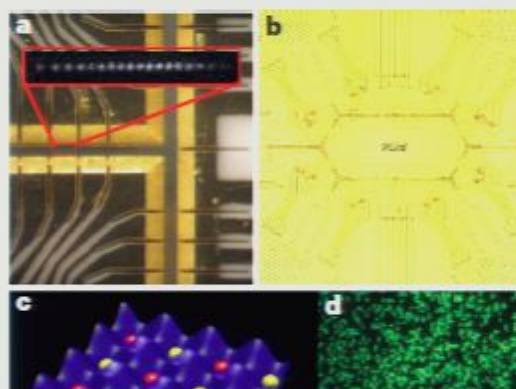
**Figure 2 | Photonic quantum computer.** A microchip containing several silica-based waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates<sup>20</sup>. Green lines show optical waveguides; yellow components are metallic contacts. Pencil tip shown for scale.

47

©2010 Macmillan Publishers Limited. All rights reserved

## REVIEWS

NATURE | Vol 464 | 4 March 2010



optical lattices for quantum computing are the controlled initialization, interaction and measurement of the atomic qubits. However, there has been much progress on all of these fronts in recent years.

Optical lattices are typically loaded with  $10^3$ – $10^6$  identical atoms, usually with non-uniform packing of lattice sites for thermal atoms. However, when a Bose condensate is loaded in an optical lattice, the competition between intrasite tunnelling and the on-site interaction between multiple atoms can result in a Mott-insulator transition where approximately the same number of atoms (for example, one) reside in every lattice site<sup>34</sup>. The interaction between atomic qubits in optical lattices can be realized in several ways. Adjacent atoms can be brought together depending on their internal qubit

laflamme-nature08812.pdf - Adobe Acrobat Pro

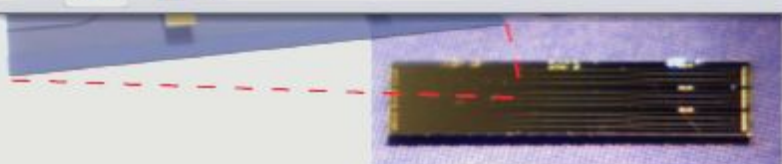
File Edit View Document Comments Forms Tools Advanced Window Help

Create Combine Collaborate Secure Sign Forms Multimedia Comment

4 / 9 105% Find

photons spontaneously<sup>18</sup>. An alternative is a single quantum system in an optical cavity that emits a single photon on transition from an excited to a ground state. Robust alignment of the cavity can be achieved with solid-state 'artificial atoms', such as quantum dots<sup>18,19,21,22</sup> and potentially with impurities in diamond<sup>23</sup>, which we discuss below. As these cavity quantum electrodynamics systems improve, they could provide deterministic photon-photon nonlinearities<sup>24</sup>.

Regardless of the approach used for photon sources, detectors and nonlinearities, photon loss remains a significant challenge, and



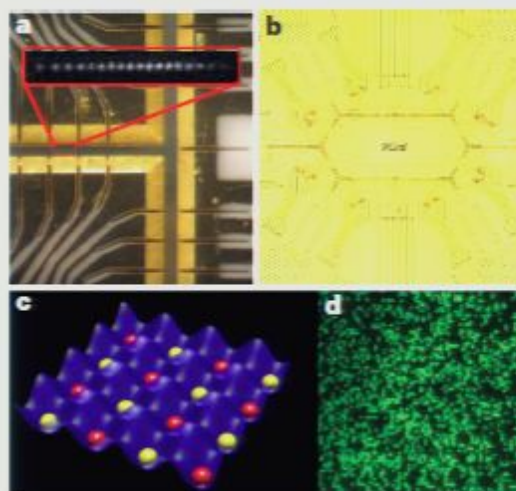
**Figure 2 | Photonic quantum computer.** A microchip containing several silica-based waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates<sup>20</sup>. Green lines show optical waveguides; yellow components are metallic contacts. Pencil tip shown for scale.

©2010 Macmillan Publishers Limited. All rights reserved

47

## REVIEWS

NATURE|Vol 464|4 March 2010



**Figure 3 | Trapped atom qubits.** a, Multi-level linear ion trap chip; the inset displays a linear crystal of several  $^{171}\text{Yb}^+$  ions fluorescing when resonant laser light is applied (the ion-ion spacing is  $4\mu\text{m}$  in the figure). Other lasers can provide qubit-state-dependent forces that can entangle the ions through their Coulomb interaction. b, Surface ion trap chip with 200 zones.

optical lattices for quantum computing are the controlled initialization, interaction and measurement of the atomic qubits. However, there has been much progress on all of these fronts in recent years.

Optical lattices are typically loaded with  $10^3$ – $10^6$  identical atoms, usually with non-uniform packing of lattice sites for thermal atoms. However, when a Bose condensate is loaded in an optical lattice, the competition between intrasite tunnelling and the on-site interaction between multiple atoms can result in a Mott-insulator transition where approximately the same number of atoms (for example, one) reside in every lattice site<sup>34</sup>. The interaction between atomic qubits in optical lattices can be realized in several ways. Adjacent atoms can be brought together depending on their internal qubit levels with appropriate laser forces, and through contact interactions, entanglement can be formed between the atoms. This approach has been exploited for the realization of entangling quantum gate operations between atoms and their neighbours<sup>35</sup>. Another approach exploits the observation that when atoms are promoted to Rydberg states, they possess very large electric dipole moments. The Rydberg 'dipole blockade' mechanism prevents more than one atom from

The scaling of trapped-ion Coulomb gates becomes difficult when large numbers of ions participate in the collective motion for several reasons: laser-cooling becomes inefficient, the ions become more susceptible to noisy electric fields and decoherence of the motional modes<sup>29</sup>, and the densely packed motional spectrum can potentially degrade quantum gates through mode crosstalk and nonlinearities<sup>25</sup>. In one promising approach to circumvent these difficulties, individual ions are shuttled between various zones of a complex trap structure through the application of controlled electrical forces from the trap electrodes. In this way, entangling gates need only operate with a small number of ions<sup>30</sup>.

Another method for scaling ion trap qubits is to couple small collections of Coulomb-coupled ions through photonic interactions, offering the advantage of having a communication channel that can easily traverse large distances. Recently, atomic ions have been entangled over macroscopic distances in this way<sup>31</sup>. This type of protocol is similar to probabilistic linear optics quantum computing schemes discussed above<sup>13</sup>, but the addition of stable qubit memories in the network allows the system to be efficiently scaled to long-distance communication through quantum repeater circuits<sup>32</sup>. Moreover, such a system can be scaled to large numbers of qubits for distributed probabilistic quantum computing<sup>33</sup>.

Neutral atoms provide qubits similar to trapped ions. An array of cold neutral atoms may be confined in free space by a pattern of crossed laser beams, forming an optical lattice<sup>34</sup>. The lasers are typically applied far from atomic resonance, and the resulting Stark shifts in the atoms provide an effective external trapping potential for the atoms. Appropriate geometries of standing-wave laser beams can result in a regular pattern of potential wells in one, two or three dimensions, with the lattice-site spacing scaled by the optical wavelength (Fig. 3c, d). Perhaps the most intriguing aspect of optical lattices is that the dimensionality, form, depth and position of optical lattices can be precisely controlled through the geometry, polarization and intensity of the external laser beams defining the lattice. The central challenges in using

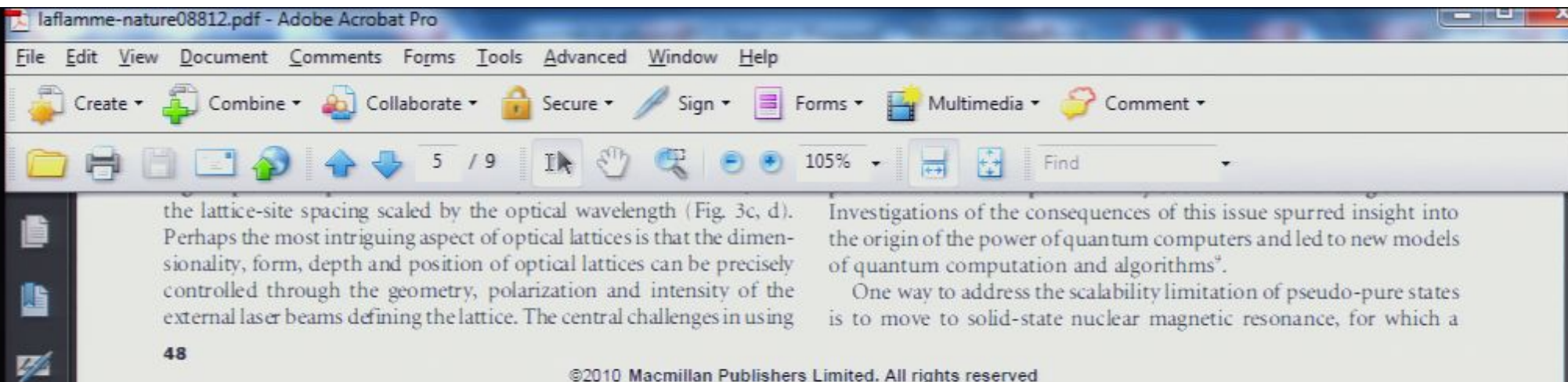
nuclear spins in molecules in liquid solutions have excellent gyroscopes; rapid molecular motion actually helps nuclei maintain their spin orientation for  $T_2$  times of many seconds, comparable to coherence times for trapped atoms. In 1996, methods were proposed<sup>6,7</sup> for building small quantum computers using these nuclear spins in conjunction with 50 years' worth of existing magnetic resonance technology.

Immersed in a strong magnetic field, nuclear spins can be identified through their Larmor frequency. In a molecule, nuclear Larmor frequencies vary from atom to atom owing to shielding effects from electrons in molecular bonds. Irradiating the nuclei with resonant radio-frequency pulses allows manipulation of nuclei of a distinct frequency, giving generic one-qubit gates. Two-qubit interactions arise from the indirect coupling mediated through molecular electrons. Measurement is achieved by observing the induced current in a coil surrounding the sample of an ensemble of such qubits.

Liquid-state nuclear magnetic resonance has allowed the manipulation of quantum processors with up to a dozen qubits<sup>38</sup>, and the implementation of algorithms<sup>39</sup> and QEC protocols. This work was enabled in large part by the development of quantum-information-inspired advances in radio-frequency pulse techniques building on the many years of engineering in magnetic resonance imaging and related technologies; these techniques continue to improve<sup>40</sup>.

Initialization is an important challenge for nuclear magnetic resonance quantum computers. The first proposals employed pseudo-pure-state techniques, which isolate the signal of an initialized pure state against a high-entropy background. However, the techniques first suggested were not scalable. Algorithmic cooling techniques<sup>8</sup> may help this problem in conjunction with additional nuclear polarization. It was also noticed that for small numbers of qubits, pseudo-pure-state-based computation may be shown to lack entanglement<sup>41</sup>. Investigations of the consequences of this issue spurred insight into the origin of the power of quantum computers and led to new models of quantum computation and algorithms<sup>9</sup>.

One way to address the scalability limitation of pseudo-pure states is to move to solid-state nuclear magnetic resonance, for which a



the lattice-site spacing scaled by the optical wavelength (Fig. 3c, d). Perhaps the most intriguing aspect of optical lattices is that the dimensionality, form, depth and position of optical lattices can be precisely controlled through the geometry, polarization and intensity of the external laser beams defining the lattice. The central challenges in using

48

©2010 Macmillan Publishers Limited. All rights reserved

Investigations of the consequences of this issue spurred insight into the origin of the power of quantum computers and led to new models of quantum computation and algorithms<sup>9</sup>.

One way to address the scalability limitation of pseudo-pure states is to move to solid-state nuclear magnetic resonance, for which a

NATURE|Vol 464|4 March 2010

REVIEWS

variety of dynamic nuclear polarization techniques exist. The lack of molecular motion allows the use of nuclear dipole–dipole couplings, which may speed up gates considerably. A recent example of a step towards solid-state nuclear magnetic resonance quantum computation can be found in the implementation of many rounds of heat-bath algorithmic cooling<sup>8</sup>. Another method of possibly extending solid-state nuclear magnetic resonance systems is to include electrons to assist in nuclear control<sup>42</sup>. These techniques have possible application to the solid-state dopants discussed in the next section.

To date, no bulk nuclear magnetic resonance technique has shown sufficient initialization or measurement capabilities for effective correctability, but nuclear magnetic resonance has led the way in many-qubit quantum control. The many-second  $T_2$  times are comparable to gate times in liquids and much longer than the sub-millisecond gate times in solids, but are still short in comparison to timescales for initialization and measurement. The many lessons learned in nuclear magnetic resonance quantum computation research are most likely to be relevant for advancing the development of other quantum technologies.

### Quantum dots and dopants in solids

A complication of quantum computing with single atoms in vacuum is the need to cool and trap them. Large arrays of qubits may be easier

A critical issue in the work described above, which was performed on dots made with group III–V semiconductors, is the inevitable presence of nuclear spins in the semiconductor substrate. Nuclear spins both create an inhomogeneous magnetic field, resulting in  $T_2^* \approx 10$  ns, and cause decoherence via dynamic spin-diffusion from the nuclear dipole–dipole interactions. This latter process limits electron spin decoherence times ( $T_2$ ) to a few microseconds<sup>43</sup>. Suppressing this decoherence requires either extraordinary levels of nuclear polarization, or the dynamic decoupling of nuclear spin noise by rapid sequences of spin rotations<sup>44</sup>.

One way to eliminate nuclear spins altogether is to use nuclear-spin-free group-IV semiconductors (that is, silicon and germanium). Many of the accomplishments demonstrated in GaAs have recently been duplicated in metal-oxide-semiconductor silicon-based<sup>45</sup> and SiGe-based quantum dots, including single electron charge sensing and the control of tunnel coupling in double dots<sup>46</sup>.

In related silicon-based proposals<sup>47,48</sup>, the quantum dot is replaced by a single impurity, in particular a single phosphorus atom, which binds a donor electron at low temperature. Quantum information may then be stored in either the donor electron, or in the state of the single  $^{31}\text{P}$  nuclear spin, accessed via the electron-nuclear hyperfine coupling. Phosphorus-bound electron spins in isotopically purified  $^{28}\text{Si}$  show encouragingly long  $T_2$  times exceeding 0.6 s, as demon-

Page 4 of 14

Printed: 11/07/2009

8:55 AM

qubit quantum control. The many-second  $T_2$  times are comparable to gate times in liquids and much longer than the sub-millisecond gate times in solids, but are still short in comparison to timescales for initialization and measurement. The many lessons learned in nuclear magnetic resonance quantum computation research are most likely to be relevant for advancing the development of other quantum technologies.

### Quantum dots and dopants in solids

A complication of quantum computing with single atoms in vacuum is the need to cool and trap them. Large arrays of qubits may be easier to assemble and cool if the 'atoms' are integrated into a solid-state host, motivating the use of quantum dots and single dopants in solids. These 'artificial atoms' occur when a small semiconductor nanostructure, impurity or impurity complex binds one or more electrons or holes (empty valence-band states) into a localized potential with discrete energy levels, which is analogous to an electron bound to an atomic nucleus.

Quantum dots come in many varieties. Some are electrostatically defined quantum dots, where the confinement is created by controlled voltages on lithographically defined metallic gates. Others are self-assembled quantum dots, where a random semiconductor growth process creates the potential for confining electrons or holes. A key difference between these two types of quantum dots is the depth of the atom-like potential they create; as a result electrostatically defined quantum dots operate at very low temperatures ( $<1$  K) and are primarily controlled electrically, whereas self-assembled quantum dots operate at higher temperatures ( $\sim 4$  K) and are primarily controlled optically.

One of the earliest proposals for quantum computation in semiconductors, that of Loss and DiVincenzo, envisioned arrays of electrostatically defined dots, each containing a single electron whose two spin states provide a qubit. Quantum logic would be accomplished by changing voltages on the electrostatic gates to move electrons closer and further from each other, activating and deactivating the exchange interaction<sup>43</sup>

Many of the accomplishments demonstrated in GaAs have recently been duplicated in metal-oxide-semiconductor silicon-based<sup>45</sup> and SiGe-based quantum dots, including single electron charge sensing and the control of tunnel coupling in double dots<sup>46</sup>.

In related silicon-based proposals<sup>47,48</sup>, the quantum dot is replaced by a single impurity, in particular a single phosphorus atom, which binds a donor electron at low temperature. Quantum information may then be stored in either the donor electron, or in the state of the single  $^{31}\text{P}$  nuclear spin, accessed via the electron-nuclear hyperfine coupling. Phosphorus-bound electron spins in isotopically purified  $^{28}\text{Si}$  show encouragingly long  $T_2$  times exceeding 0.6 s, as demonstrated by electron-spin resonance<sup>49</sup>. The potential for nuclear spin decoherence times of minutes or longer has further been seen in nuclear magnetic resonance dynamic decoupling experiments<sup>50</sup> with  $^{29}\text{Si}$  in  $^{28}\text{Si}$ . Isotopically purified silicon also shows optical transitions related to the  $^{31}\text{P}$  donor that are extremely sharp in comparison to other optical solid-state systems, revealing inhomogeneous broadening comparable to the 60-MHz hyperfine coupling. These transitions enable rapid (less than 1 s) electron and nuclear spin polarization by optical pumping<sup>51</sup>. Recently, silicon-based transistors have aided the detection of the ion-implantation of single dopants<sup>52</sup>, a technique which adds to scanning tunnelling microscopy techniques<sup>53</sup> for placing phosphorus impurities in prescribed atomic locations.

However, a challenge in using electrostatically defined quantum dots or silicon-based impurities for quantum computation is that the exchange interaction is extremely short-range, imposing a substantial constraint when considering the requirements of fault-tolerant QEC. As with trapped ions and atoms, photonic connections between quantum dots may help to resolve this issue. Self-assembled quantum dots are particularly useful for these connections because their large size in comparison to single atoms increases their coupling to photons.

The development of self-assembled dots is hindered by their random nature; they form in random locations and, unlike atoms, their optical characteristics vary from dot to dot. Emerging fabrication techniques for deterministic placement of dots<sup>54</sup> and dot tuning techniques<sup>55</sup>

single electron charge; to measure a spin, the ability of a single electron to tunnel into or out of a quantum dot is altered according to its spin state<sup>43</sup>. The control of individual spins has also been demonstrated via direct generation of microwave magnetic and electric fields. These techniques have allowed measurement of  $T_2^*$  and  $T_2$  times by spin-echo techniques. Qubits may also be defined by clusters of exchange-coupled spins, with effective single-qubit logic controlled by the pairwise exchange interaction. Voltage control of a multi-electron qubit via the exchange interaction has the particular advantage of being faster than direct microwave transitions. The  $T_2$  decoherence of a qubit defined by an exchange-coupled electron pair was measured this way<sup>43</sup>.

quantum computers.

Optically active solid-state dopants also allow photonic connections, but with greater optical homogeneity. The negatively charged nitrogen-vacancy centre in diamond (Fig. 4c) is one such dopant. It consists of a substitutional nitrogen at a lattice site neighbouring a missing carbon atom. The negatively charged state of the nitrogen-vacancy centre forms a triplet spin system. Under optical illumination, spin-selective relaxations facilitate efficient optical pumping of the system into a single spin state, allowing fast (250 ns) initialization of the spin qubit<sup>49</sup>. The spin state of a nitrogen-vacancy centre may then be coherently manipulated with resonant microwave fields<sup>60</sup>, and then detected in a few milliseconds via spin-dependent

©2010 Macmillan Publishers Limited. All rights reserved

49

## REVIEWS

NATURE | Vol 464 | 4 March 2010

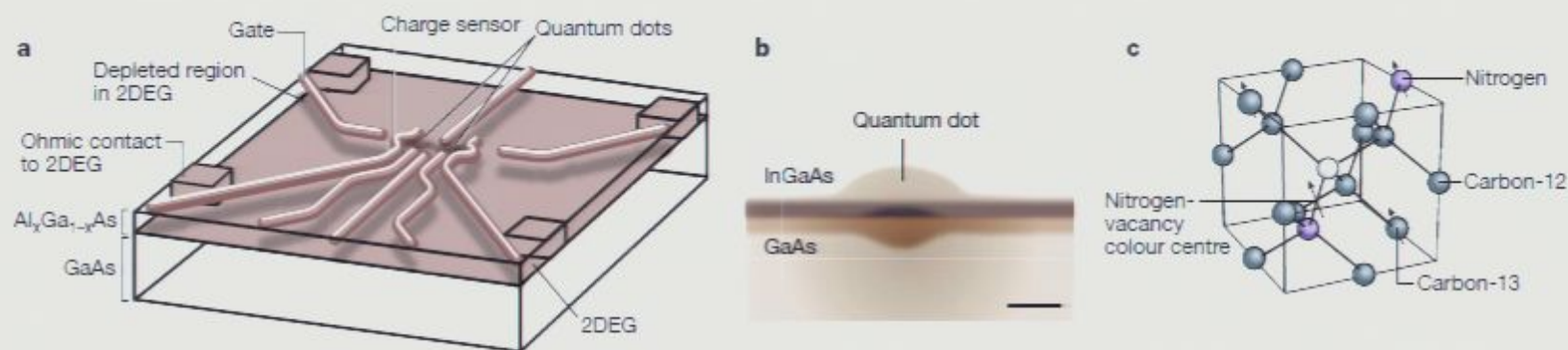


Figure 4 | Quantum dot and solid-state dopant qubits. a, An

dot. Scale bar, ~5 nm. c, The atomic structure of a nitrogen-vacancy centre

strated via direct generation of microwave magnetic and electric fields. These techniques have allowed measurement of  $T_2^*$  and  $T_2$  times by spin-echo techniques. Qubits may also be defined by clusters of exchange-coupled spins, with effective single-qubit logic controlled by the pairwise exchange interaction. Voltage control of a multi-electron qubit via the exchange interaction has the particular advantage of being faster than direct microwave transitions. The  $T_2$  decoherence of a qubit defined by an exchange-coupled electron pair was measured this way<sup>43</sup>.

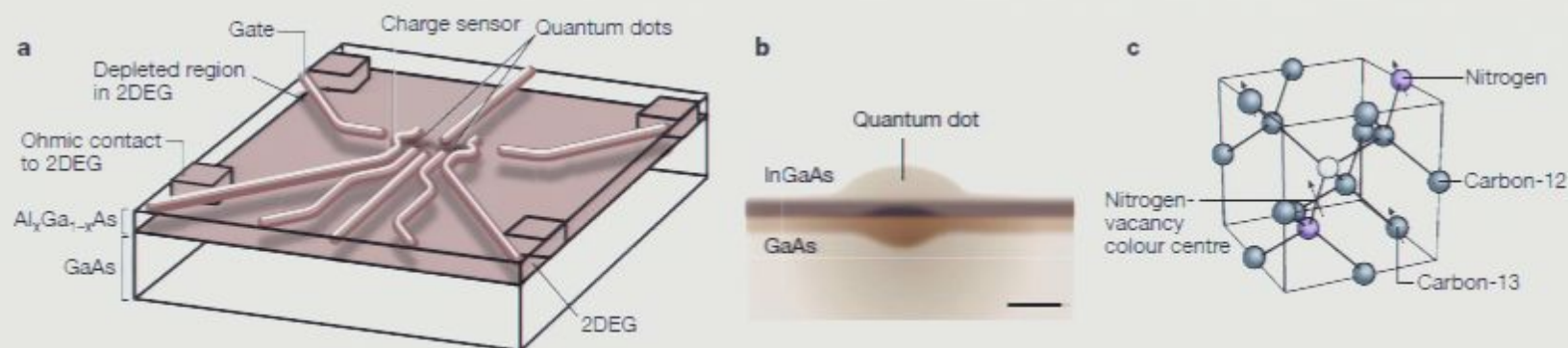
nitrogen-vacancy centre in diamond (Fig. 4c) is one such dopant. It consists of a substitutional nitrogen at a lattice site neighbouring a missing carbon atom. The negatively charged state of the nitrogen-vacancy centre forms a triplet spin system. Under optical illumination, spin-selective relaxations facilitate efficient optical pumping of the system into a single spin state, allowing fast (250 ns) initialization of the spin qubit<sup>49</sup>. The spin state of a nitrogen-vacancy centre may then be coherently manipulated with resonant microwave fields<sup>50</sup>, and then detected in a few milliseconds via spin-dependent

49

©2010 Macmillan Publishers Limited. All rights reserved

## REVIEWS

NATURE | Vol 464 | 4 March 2010



**Figure 4 | Quantum dot and solid-state dopant qubits.** **a**, An electrostatically confined quantum dot; the structure shown is several  $\mu\text{m}$  across. 2DEG, two-dimensional electron gas. **b**, A self-assembled quantum

dot. Scale bar,  $\sim 5\text{ nm}$ . **c**, The atomic structure of a nitrogen-vacancy centre in the diamond lattice, with lattice constant  $3.6\text{ \AA}$ . Figure copied from figure 1 of ref. 111 with permission.

magnetic ground state similar to that in nitrogen-vacancy defects<sup>7</sup>. In the wide-gap, group II–VI semiconductor ZnSe, the fluorine impurity has a similar binding energy and spin structure to that of phosphorus in silicon and a comparable potential for isotopic depletion of nuclear spins from the substrate. Unlike silicon- or diamond-based impurities, it has an oscillator strength comparable to that of a quantum dot<sup>70</sup>.

Although it is routine to make large wafers of spins trapped in dots and impurities, scaling a system of coupled spins remains a challenge. The microsecond  $T_2$  times seen in GaAs are long in comparison to their 1–100-ps qubit control times and 1–10-ns measurement and

flux and phase—with potentials shown in Fig. 5b–d. A critical difference between the different qubit types is the ratio  $E_J/E_C$ , where  $E_C = e^2/2C$  is the single electron charging energy characterizing the charging effect, that is, the kinetic term. This ratio alters the nature of the wavefunctions and their sensitivity to charge and flux fluctuations.

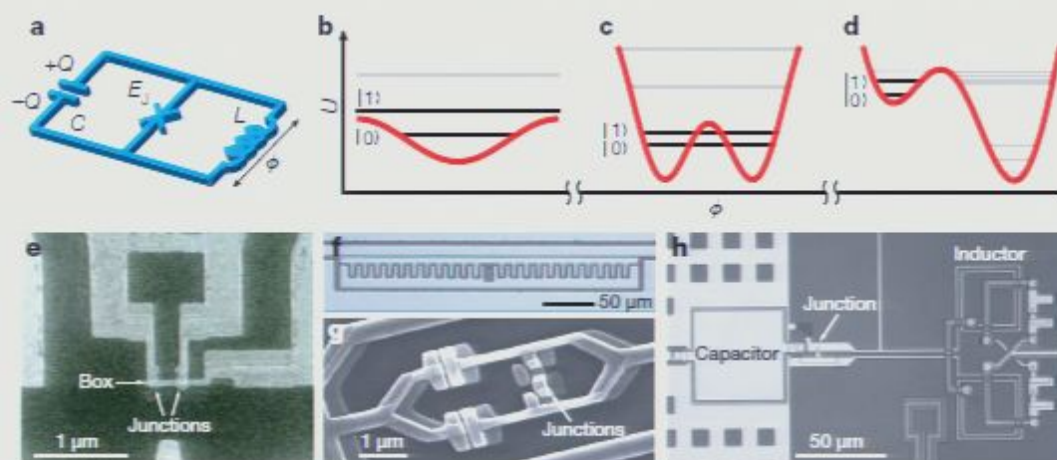
The first type of superconducting qubit, the charge qubit, omits the inductance. There is no closed superconducting loop, and the potential is simply a cosine with a minimum at zero phase. It is sometimes called a Cooper-pair box, because it relies ultimately on the quantization of charge into individual Cooper pairs, which becomes a dominant effect when a sufficiently small ‘box’ electrode

50

©2010 Macmillan Publishers Limited. All rights reserved

NATURE|Vol 464|4 March 2010

REVIEWS



**Figure 5 | Superconducting qubits.** **a**, Minimal circuit model of superconducting qubits. The Josephson junction is denoted by the blue 'X'. **b–d**, Potential energy  $U(\phi)$  (red) and qubit energy levels (black) for charge (**b**), flux (**c**), and phase qubits (**d**), respectively. **e–h**, Micrographs of

junctions consist of  $\text{Al}_2\text{O}_3$  tunnel barriers between two layers of Al. **e**, Charge qubit, or a Cooper pair box. **f**, Transmon, a derivative of charge qubit with large  $E_J/E_C$  (courtesy of R. J. Schoelkopf). The Josephson junction in the middle is not visible at this scale. **g**, Flux qubit (courtesy of J. E. Mooij).

the wide-gap, group II-VI semiconductor ZnSe, the nitrogen impurity has a similar binding energy and spin structure to that of phosphorus in silicon and a comparable potential for isotopic depletion of nuclear spins from the substrate. Unlike silicon- or diamond-based impurities, it has an oscillator strength comparable to that of a quantum dot<sup>70</sup>.

Although it is routine to make large wafers of spins trapped in dots and impurities, scaling a system of coupled spins remains a challenge. The microsecond  $T_2$  times seen in GaAs are long in comparison to their 1–100-ps qubit control times and 1–10-ns measurement and

ence between the different qubit types is the ratio  $E_J/E_C$ , where  $E_C = e^2/2C$  is the single electron charging energy characterizing the charging effect, that is, the kinetic term. This ratio alters the nature of the wavefunctions and their sensitivity to charge and flux fluctuations.

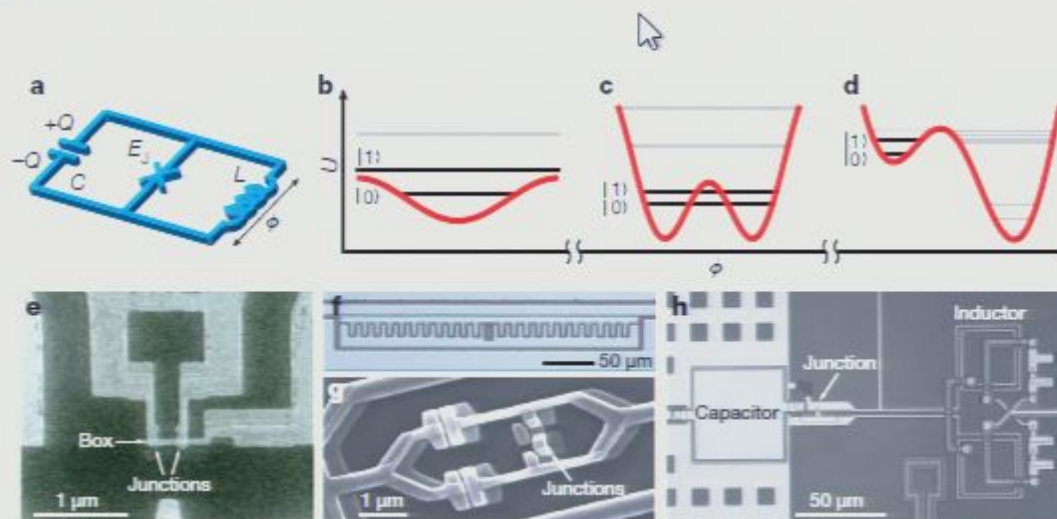
The first type of superconducting qubit, the charge qubit, omits the inductance. There is no closed superconducting loop, and the potential is simply a cosine with a minimum at zero phase. It is sometimes called a Cooper-pair box, because it relies ultimately on the quantization of charge into individual Cooper pairs, which becomes a dominant effect when a sufficiently small ‘box’ electrode

50

©2010 Macmillan Publishers Limited. All rights reserved

NATURE | Vol 464 | 4 March 2010

REVIEWS

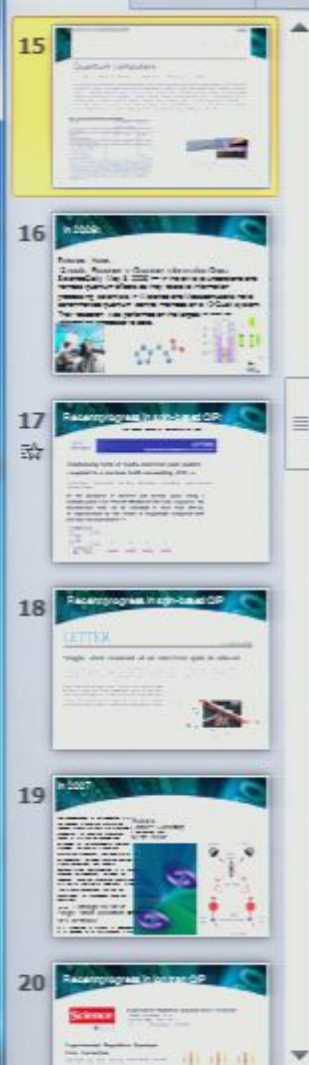


**Figure 5 | Superconducting qubits.** **a**, Minimal circuit model of superconducting qubits. The Josephson junction is denoted by the blue ‘X’. **b–d**, Potential energy  $U(\phi)$  (red) and qubit energy levels (black) for charge (**b**), flux (**c**), and phase qubits (**d**), respectively. **e–h**, Micrographs of superconducting qubits. The circuits are made of Al films. The Josephson

junctions consist of  $\text{Al}_2\text{O}_3$  tunnel barriers between two layers of Al. **e**, Charge qubit, or a Cooper pair box. **f**, Transmon, a derivative of charge qubit with large  $E_J/E_C$  (courtesy of R. J. Schoelkopf). The Josephson junction in the middle is not visible at this scale. **g**, Flux qubit (courtesy of J. E. Martinis). **h**, Phase qubit (courtesy of J. M. Martinis).



Slides Outline X



Vol 464/4 March 2010 | doi:10.1038/nature08812

nature

## REVIEWS

## Quantum computers

T. D. Ladd<sup>1</sup>†, F. Jelezko<sup>2</sup>, R. Laflamme<sup>3,4,5</sup>, Y. Nakamura<sup>6,7</sup>, C. Monroe<sup>8,9</sup> & J. L. O'Brien<sup>10</sup>

Over the past several decades, quantum information science has emerged to seek answers to the question: can we gain some advantage by storing, transmitting and processing information encoded in systems that exhibit unique quantum properties? Today it is understood that the answer is yes, and many research groups around the world are working towards the highly ambitious technological goal of building a quantum computer, which would dramatically improve computational power for particular tasks. A number of physical systems, spanning much of modern physics, are being developed for quantum computation. However, it remains unclear which technology, if any, will ultimately prove successful. Here we describe the latest developments for each of the leading approaches and explain the major challenges for the future.

Table 1 | Current performance of various qubits

Type of qubit	$T_1$	Benchmarking (%)		References
		One qubit	Two qubits	
Infrared photon	0.1 ms	0.016	1	20
Trapped ion	15 s	0.48 <sup>†</sup>	0.7*	104–106
Trapped neutral atom	3 s	5		107
Liquid molecule nuclear spins	2 s	0.01 <sup>†</sup>	0.47 <sup>†</sup>	108
$e^-$ spin in GaAs quantum dot	3 $\mu$ s	5		43, 57
$e^-$ spins bound to $^{29}\text{Si}$	0.6 s	5		49
$^{29}\text{Si}$ nuclear spins in $^{29}\text{Si}$	25 s	5		50
NV centre in diamond	2 ms	2	5	60, 61, 65
Superconducting circuit	4 $\mu$ s	0.7 <sup>†</sup>	10*	73, 79, 81, 109

Measured  $T_1$  times are shown, except for photons where  $T_1$  is replaced by twice the hold time (comparable to  $T_1$ ) of a telecommunication-wavelength photon in fibre. Benchmarking values show approximate error rates for single or multi-qubit gates. Values marked with asterisks are found by quantum process or state tomography, and give the departure of the fidelity from 100%. Values marked with daggers are found with randomized benchmarking<sup>60</sup>. Other values are rough experimental gate error estimates. In the case of photons, two-qubit gates fail frequently but success is heralded; error rates shown are conditional on a heralded success. NV, nitrogen vacancy.

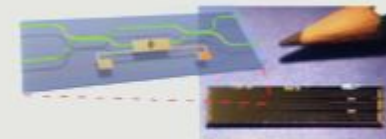


Figure 2 | Photonic quantum computer. A microchip containing several silica-based waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates<sup>61</sup>. Green lines show optical waveguides, yellow components are metal contacts. Pencil tip shows for scale.

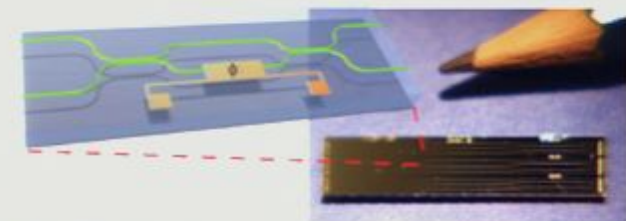
Click to add notes

particular tasks. A number of physical systems, spanning much of modern physics, are being developed for quantum computation. However, it remains unclear which technology, if any, will ultimately prove successful. Here we describe the latest developments for each of the leading approaches and explain the major challenges for the future.

**Table 1 | Current performance of various qubits**

Type of qubit	$T_2$	Benchmarking (%)		References
		One qubit	Two qubits	
Infrared photon	0.1 ms	0.016	1	20
Trapped ion	15 s	0.48 <sup>†</sup>	0.7*	104–106
Trapped neutral atom	3 s	5		107
Liquid molecule nuclear spins	2 s	0.01 <sup>†</sup>	0.47 <sup>†</sup>	108
e <sup>−</sup> spin in GaAs quantum dot	3 $\mu$ s	5		43, 57
e <sup>−</sup> spins bound to <sup>31</sup> P: <sup>28</sup> Si	0.6 s	5		49
<sup>29</sup> Si nuclear spins in <sup>28</sup> Si	25 s	5		50
NV centre in diamond	2 ms	2	5	60, 61, 65
Superconducting circuit	4 $\mu$ s	0.7 <sup>†</sup>	10*	73, 79, 81, 109

Measured  $T_2$  times are shown, except for photons where  $T_2$  is replaced by twice the hold-time (comparable to  $T_1$ ) of a telecommunication-wavelength photon in fibre. Benchmarking values show approximate error rates for single or multi-qubit gates. Values marked with asterisks are found by quantum process or state tomography, and give the departure of the fidelity from 100%. Values marked with daggers are found with randomized benchmarking<sup>10</sup>. Other values are rough experimental gate error estimates. In the case of photons, two-qubit gates fail frequently but success is heralded; error rates shown are conditional on a heralded success. NV, nitrogen vacancy.



**Figure 2 | Photonic quantum computer.** A microchip containing several silica-based waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates<sup>20</sup>. Green lines show optical waveguides; yellow components are metallic contacts. Pencil tip shown for scale.

## REVIEWS

## Quantum computers

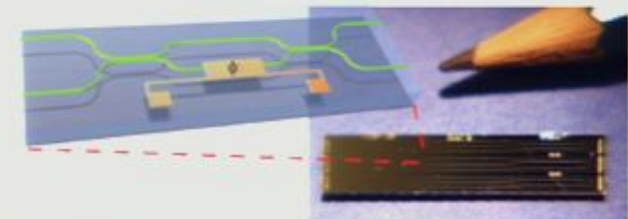
T. D. Ladd<sup>1†</sup>, F. Jelezko<sup>2</sup>, R. Laflamme<sup>3,4,5</sup>, Y. Nakamura<sup>6,7</sup>, C. Monroe<sup>8,9</sup> & J. L. O'Brien<sup>10</sup>

Over the past several decades, quantum information science has emerged to seek answers to the question: can we gain some advantage by storing, transmitting and processing information encoded in systems that exhibit unique quantum properties? Today it is understood that the answer is yes, and many research groups around the world are working towards the highly ambitious technological goal of building a quantum computer, which would dramatically improve computational power for particular tasks. A number of physical systems, spanning much of modern physics, are being developed for quantum computation. However, it remains unclear which technology, if any, will ultimately prove successful. Here we describe the latest developments for each of the leading approaches and explain the major challenges for the future.

**Table 1 | Current performance of various qubits**

Type of qubit	$T_2$	Benchmarking (%)		References
		One qubit	Two qubits	
Infrared photon	0.1 ms	0.016	1	20
Trapped ion	15 s	0.48 <sup>†</sup>	0.7*	104–106
Trapped neutral atom	3 s	5		107
Liquid molecule nuclear spins	2 s	0.01 <sup>†</sup>	0.47 <sup>†</sup>	108
$e^-$ spin in GaAs quantum dot	3 $\mu$ s	5		43, 57
$e^-$ spins bound to $^{31}\text{P}$ : $^{28}\text{Si}$	0.6 s	5		49
$^{29}\text{Si}$ nuclear spins in $^{28}\text{Si}$	25 s	5		50
NV centre in diamond	2 ms	2	5	60, 61, 65
Superconducting circuit	4 $\mu$ s	0.7 <sup>†</sup>	10*	73, 79, 81, 109

Measured  $T_2$  times are shown, except for photons where  $T_2$  is replaced by twice the hold-time (comparable to  $T_2$ ) of a telecommunication-wavelength photon in fibre. Benchmarking values show approximate error rates for single or multi-qubit gates. Values marked with asterisks are found by quantum process or state tomography, and give the departure of the fidelity from 100%. Values marked with daggers are found with randomized benchmarking<sup>90</sup>. Other values are rough experimental gate error estimates. In the case of photons, two-qubit gates fail frequently but success is heralded; error rates shown are conditional on a heralded success. NV, nitrogen vacancy.



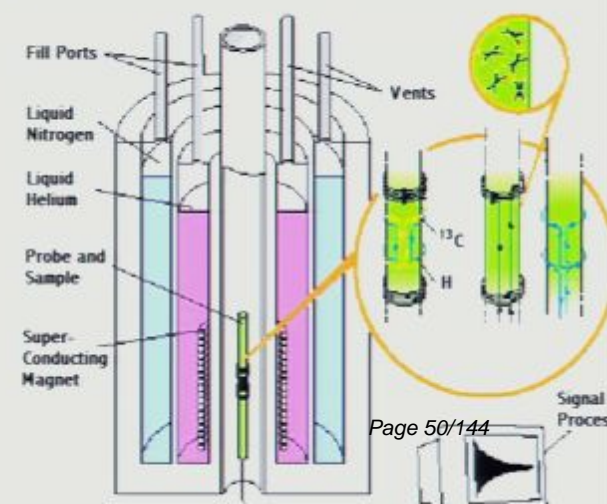
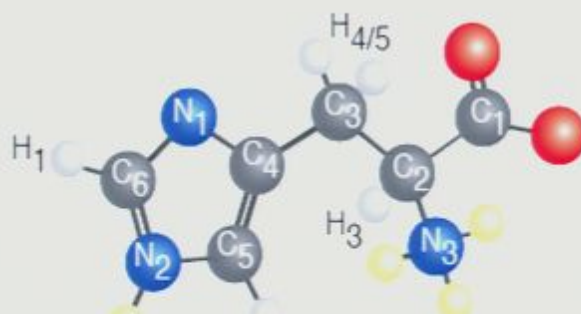
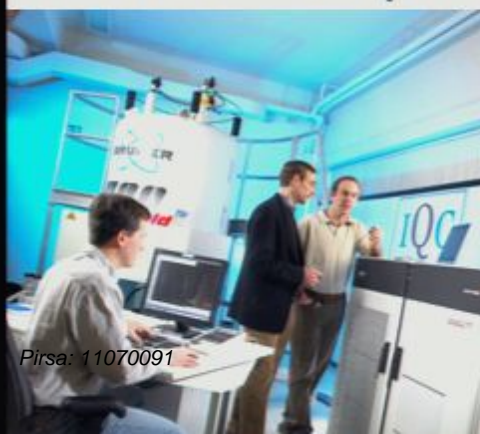
**Figure 2 | Photonic quantum computer.** A microchip containing several silica-based waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates<sup>91</sup>. Green lines show optical waveguides; yellow components are metallic contacts. Pencil tip shown for scale.

In 2006:

## Science News

### 12-qubits Reached In Quantum Information Quest

ScienceDaily (May 8, 2006) — In the drive to understand and harness quantum effects as they relate to information processing, scientists in Waterloo and Massachusetts have benchmarked quantum control methods on a 12-Qubit system. Their research was performed on the largest quantum information processor to date.



# Recent progress in spin-based QIP:

*(see Wang, Rochette, Bureau-Oxton talks)*

# Recent progress in spin-based QIP:

(see Wang, Rochette, Bureau-Oxton talks)

nature  
physics

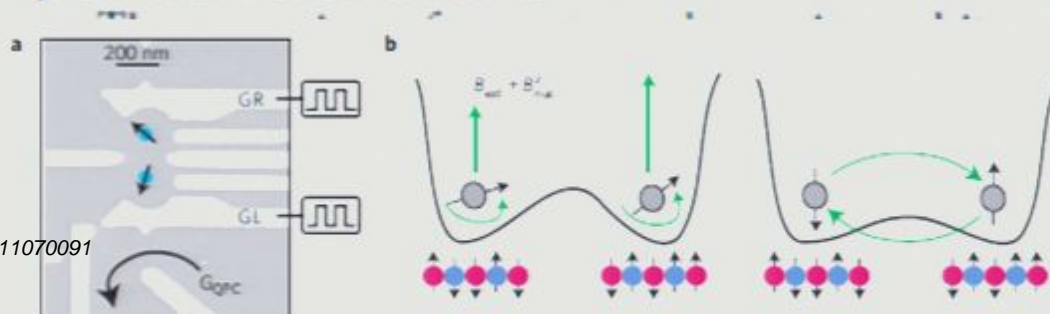
LETTERS

PUBLISHED ONLINE: 12 DECEMBER 2010 | DOI: 10.1038/NPHYS1856

## Dephasing time of GaAs electron-spin qubits coupled to a nuclear bath exceeding $200\ \mu\text{s}$

Hendrik Bluhm<sup>1†</sup>, Sandra Foletti<sup>1†</sup>, Izhar Neder<sup>1</sup>, Mark Rudner<sup>1</sup>, Diana Mahalu<sup>2</sup>, Vladimir Umansky<sup>2</sup> and Amir Yacoby<sup>1\*</sup>

for the dynamics of electron and nuclear spins. Using a multiple-pulse Carr-Purcell-Meiboom-Gill echo sequence, the decoherence time can be extended to more than  $200\ \mu\text{s}$ , an improvement by two orders of magnitude compared with previous measurements<sup>1,2,5</sup>.



# Recent progress in spin-based QIP

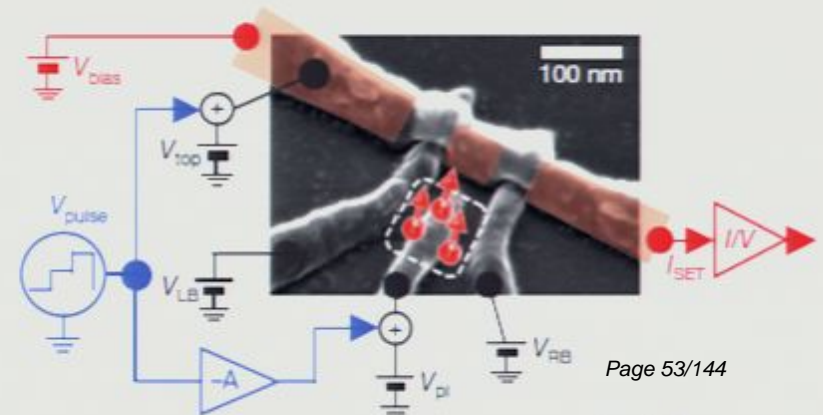
## LETTER

doi:10.1038/nature09392

### Single-shot readout of an electron spin in silicon

Andrea Morello<sup>1</sup>, Jarryd J. Pla<sup>1</sup>, Floris A. Zwanenburg<sup>1</sup>, Kok W. Chan<sup>1</sup>, Kuan Y. Tan<sup>1</sup>, Hans Huebl<sup>1†</sup>, Mikko Möttönen<sup>1,3,4</sup>, Christopher D. Nugroho<sup>1†</sup>, Changyi Yang<sup>2</sup>, Jessica A. van Donkelaar<sup>2</sup>, Andrew D. C. Alves<sup>2</sup>, David N. Jamieson<sup>2</sup>, Christopher C. Escott<sup>1</sup>, Lloyd C. L. Hollenberg<sup>2</sup>, Robert G. Clark<sup>1†</sup> & Andrew S. Dzurak<sup>1</sup>

nuclear spins from the bulk crystal<sup>8</sup>. However, the control of single electrons in silicon has proved challenging, and so far the observation and manipulation of a single spin has been impossible. Here we report the demonstration of single-shot, time-resolved readout of an electron spin in silicon. This has been performed in a device



In 2007

The phenomenon of entanglement is a key concept in quantum information science. Atomic systems are promising candidates for quantum 'memories'. These in turn can be coupled and entangled by the exchange of photons, providing the basis of a quantum information processor. The signature of entanglement between remotely located atomic ensembles was recently demonstrated. Now Moehring *et al.* have achieved entanglement between two single-ion quantum memories separated by a metre. The use of single ions, rather than atomic ensembles, has certain advantages for subsequent quantum operations.

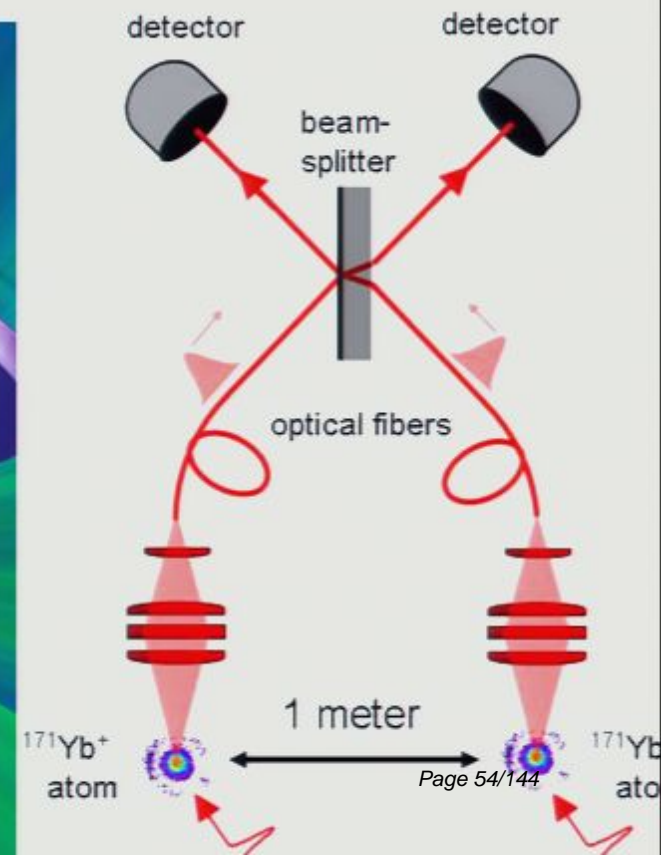
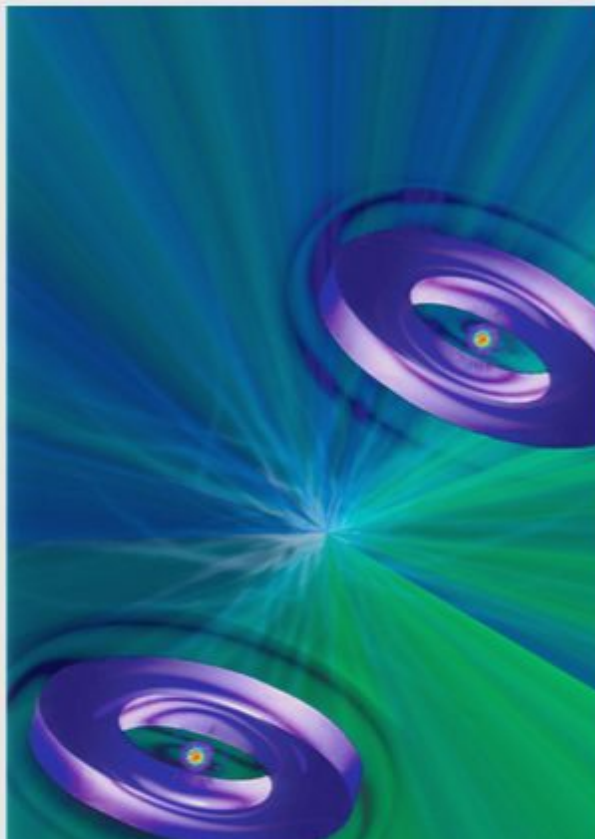
### Letter: **Entanglement of single-atom quantum bits at a distance**

D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M.

## Nature Editor's Summary

6 September 2007

### Metre made



# Recent progress in ion trap QIP



## Experimental Repetitive Quantum Error Correction

Philipp Schindler, *et al.*

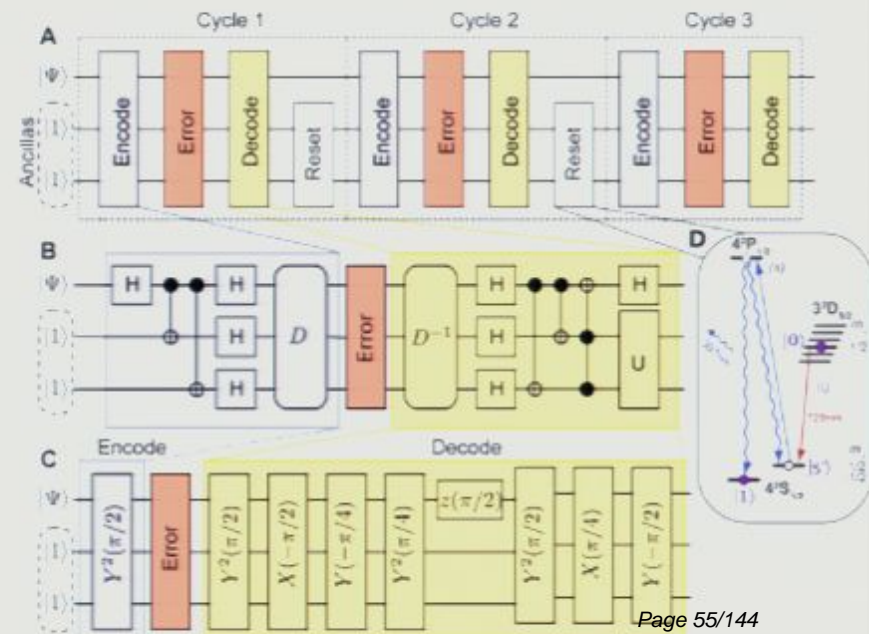
*Science* **332**, 1059 (2011);

DOI: 10.1126/science.1203329

## Experimental Repetitive Quantum Error Correction

Philipp Schindler,<sup>1</sup> Julio T. Barreiro,<sup>1</sup> Thomas Monz,<sup>1</sup> Volckmar Nebendahl,<sup>2</sup> Daniel Nigg,<sup>1</sup> Michael Chwalla,<sup>1,3</sup> Markus Hennrich,<sup>1\*</sup> Rainer Blatt<sup>1,3</sup>

The computational potential of a quantum processor can only be unleashed if errors during a quantum computation can be controlled and corrected for. Quantum error correction works if imperfections of quantum gate operations and measurements are below a certain threshold and corrections can be applied repeatedly. We implement multiple quantum error correction cycles for phase-flip errors on qubits encoded with trapped ions. Errors are corrected by a quantum-feedback algorithm using high-fidelity gate operations and a reset technique for the auxiliary qubits. Up to three consecutive correction cycles are realized, and the behavior of the algorithm for different noise environments is analyzed.



# Recent progress in ion trap QIP

PRL **106**, 130506 (2011)

PHYSICAL REVIEW LETTERS

week ending  
1 APRIL 2011

## 14-Qubit Entanglement: Creation and Coherence

Thomas Monz,<sup>1</sup> Philipp Schindler,<sup>1</sup> Julio T. Barreiro,<sup>1</sup> Michael Chwalla,<sup>1</sup> Daniel Nigg,<sup>1</sup> William A. Coish,<sup>2,3</sup>  
Maximilian Harlander,<sup>1</sup> Wolfgang Hänsel,<sup>4</sup> Markus Hennrich,<sup>1,\*</sup> and Rainer Blatt<sup>1,4</sup>

<sup>1</sup>*Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria*

<sup>2</sup>*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo,  
Waterloo, ON, N2L 3G1, Canada*

<sup>3</sup>*Department of Physics, McGill University, Montreal, Quebec, Canada H3A 2T8*

<sup>4</sup>*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften,  
Otto-Hittmair-Platz 1, A-6020 Innsbruck, Austria*

(Received 30 September 2010; published 31 March 2011)

We report the creation of Greenberger-Horne-Zeilinger states with up to 14 qubits. By investigating the coherence of up to 8 ions over time, we observe a decay proportional to the square of the number of qubits. The observed decay agrees with a theoretical model which assumes a system affected by correlated, Gaussian phase noise. This model holds for the majority of current experimental systems developed towards quantum computation and quantum metrology.

DOI: 10.1103/PhysRevLett.106.130506

PACS numbers: 03.67.Mn, 03.65.Ud, 32.80.Qk, 37.10.Ty

# Recent progress in entangling stationary and optical qubits

nature

Vol 466 | 5 August 2010 | doi:10.1038/nature09256

## LETTERS

### Quantum entanglement between an optical photon and a solid-state spin qubit

E. Togan<sup>1\*</sup>, Y. Chu<sup>1\*</sup>, A. S. Trifonov<sup>1</sup>, L. Jiang<sup>1,2,3</sup>, J. Maze<sup>1</sup>, L. Childress<sup>1,4</sup>, M. V. G. Dutt<sup>1,5</sup>, A. S. Sørensen<sup>6</sup>, P. R. Hemmer<sup>7</sup>, A. S. Zibrov<sup>1</sup> & M. D. Lukin<sup>1</sup>

high degree of control over interactions between a solid-state qubit and the quantum light field can be achieved. The reported entanglement source can be used in studies of fundamental quantum phenomena and provides a key building block for the solid-state realization of quantum optical networks<sup>1,3,14</sup>.

A quantum network<sup>13</sup> consists of several nodes, each containing a

# Recent progress in entangling stationary and optical qubits

nature

Vol 466 | 5 August 2010 | doi:10.1038/nature09256

## LETTERS

### Quantum entanglement between an optical photon and a solid-state spin qubit

E. Togan<sup>1\*</sup>, Y. Chu<sup>1\*</sup>, A. S. Trifonov<sup>1</sup>, L. Jiang<sup>1,2,3</sup>, J. Maze<sup>1</sup>, L. Childress<sup>1,4</sup>, M. V. G. Dutt<sup>1,5</sup>, A. S. Sørensen<sup>6</sup>, P. R. Hemmer<sup>7</sup>, A. S. Zibrov<sup>1</sup> & M. D. Lukin<sup>1</sup>

high degree of control over interactions between a solid-state qubit and the quantum light field can be achieved. The reported entanglement source can be used in studies of fundamental quantum phenomena and provides a key building block for the solid-state realization of quantum optical networks<sup>1,3,14</sup>.

A quantum network<sup>13</sup> consists of several nodes, each containing a

In 2007

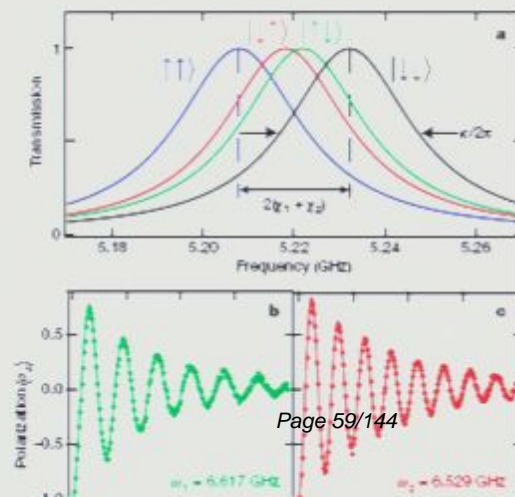
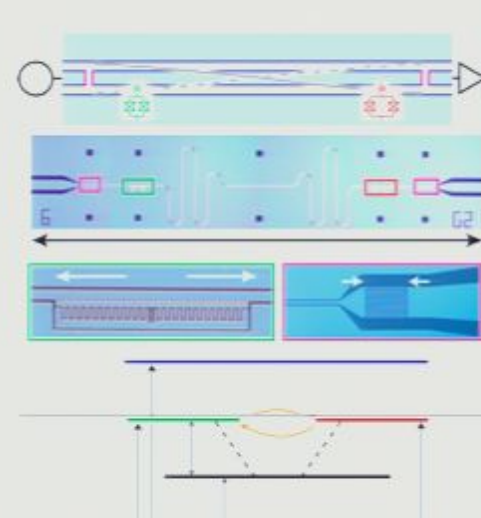


Volume 449 Number 7161

In this issue (27 September 2007)

Coupling superconducting qubits via a cavity bus

J. Majer et al., Yale University, ETH Zurich, Université de Sherbrooke



# Recent progress in superconducting QIP

nature

Vol 460 | 9 July 2009 | doi:10.1038/nature08121

## LETTERS

---

### Demonstration of two-qubit algorithms with a superconducting quantum processor

L. DiCarlo<sup>1</sup>, J. M. Chow<sup>1</sup>, J. M. Gambetta<sup>2</sup>, Lev S. Bishop<sup>1</sup>, B. R. Johnson<sup>1</sup>, D. I. Schuster<sup>1</sup>, J. Majer<sup>3</sup>, A. Blais<sup>4</sup>, L. Frunzio<sup>1</sup>, S. M. Girvin<sup>1</sup> & R. J. Schoelkopf<sup>1</sup>

## LETTER

doi:10.1038/nature09416

---

---

### Preparation and measurement of three-qubit entanglement in a superconducting circuit

L. DiCarlo<sup>1</sup>, M. D. Reed<sup>1</sup>, L. Sun<sup>1</sup>, B. R. Johnson<sup>1</sup>, J. M. Chow<sup>1</sup>, J. M. Gambetta<sup>2</sup>, L. Frunzio<sup>1</sup>, S. M. Girvin<sup>1</sup>, M. H. Devoret<sup>1</sup> & R. J. Schoelkopf<sup>1</sup>

# Recent progress in superconducting QIP

## LETTER

doi:10.1038/nature09418

### Generation of three-qubit entangled states using superconducting phase qubits

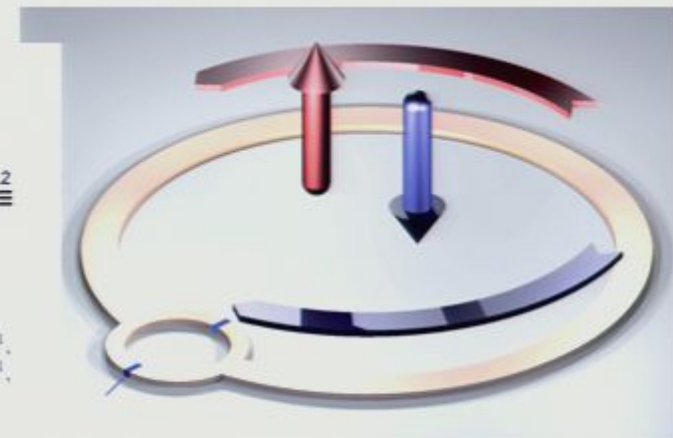
Matthew Neeley<sup>1</sup>, Radoslaw C. Bialczak<sup>1</sup>, M. Lenander<sup>1</sup>, E. Lucero<sup>1</sup>, Matteo Mariantoni<sup>1</sup>, A. D. O'Connell<sup>1</sup>, D. Sank<sup>1</sup>, H. Wang<sup>1</sup>, M. Weides<sup>1</sup>, J. Wenner<sup>1</sup>, Y. Yin<sup>1</sup>, T. Yamamoto<sup>1,2</sup>, A. N. Cleland<sup>1</sup> & John M. Martinis<sup>1</sup>

## LETTER

doi:10.1038/nature10012

### Quantum annealing with manufactured spins

M. W. Johnson<sup>1</sup>, M. H. S. Amin<sup>1</sup>, S. Gildert<sup>1</sup>, T. Lanting<sup>1</sup>, F. Hamze<sup>1</sup>, N. Dickson<sup>1</sup>, R. Harris<sup>1</sup>, A. J. Berkley<sup>1</sup>, J. Johansson<sup>2</sup>, P. Bunyk<sup>1</sup>, E. M. Chapple<sup>1</sup>, C. Enderud<sup>1</sup>, J. P. Hilton<sup>1</sup>, K. Karimi<sup>1</sup>, E. Ladizinsky<sup>1</sup>, N. Ladizinsky<sup>1</sup>, T. Oh<sup>1</sup>, I. Perminov<sup>1</sup>, C. Rich<sup>1</sup>, M. C. Thom<sup>1</sup>, E. Tolkacheva<sup>1</sup>, C. J. S. Truncik<sup>1</sup>, S. Uchaikin<sup>1</sup>, J. Wang<sup>1</sup>, B. Wilson<sup>1</sup> & G. Rose<sup>1</sup>



Any progress in developing new quantum algorithms?

YES!



Any progress in developing new quantum algorithms?

# Any progress in developing new quantum algorithms?

YES!

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

## Quantum algorithms for algebraic problems

Andrew M. Childs<sup>1</sup>

Department of Combinatorics & Optimization and Institute for Quantum Computing  
University of Waterloo, Waterloo, Ontario, Canada N2L 2G1

Mark van Dam<sup>2</sup>

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

Quantum computers use physical algorithms that fundamentally supersede classical computation. In the few decades elapsed, they have opened up efficient quantum algorithms for factoring, discrete logarithms, and many other problems that are difficult for classical computers. Understanding what other computational problems can be solved significantly better using quantum algorithms is one of the most challenges in the theory of quantum computation, and such algorithms motivate the fundamental task of finding a rigorous quantum complexity theory. This article reviews the current state of quantum complexity, focusing on algorithms with superpolynomial speedups over classical computation, and in particular on problems with an algebraic flavor.

MSC numbers: 68Q14

Contents	
I. Introduction	1
II. Complexity of Quantum Computation	2
A. Quantum data	2
B. Quantum circuits	2
C. Algorithmic complexity	2
D. Quantum complexity theory	2
E. Fast algorithms	2
III. Abelian Quantum Fourier Transforms	3
A. Fourier transforms over finite Abelian groups	3
B. Efficient quantum circuits for the QFT over $\mathbb{Z}_2^k$	3
C. Phase estimation and the QFT over real and finite Abelian groups	3
D. The QFT over a finite field	3
IV. Abelian Hidden Subgroup Problems	4
A. General setting over $\mathbb{Z}_2^k$	4
B. Computing discrete logarithms	4
C. Discrete logarithms and cryptography	4
D. The $q$ -SVP problem and the QFT over $\mathbb{Z}_q$	4
E. Hidden subgroup problems for finite Abelian groups	4
F. Period finding over $\mathbb{Z}$	4
G. Factoring integers	4
H. Breaking elliptic curve cryptography	4
I. Determining Abelian and non-Abelian groups	4
J. Computing primes in groups	4
V. Quantum Algorithms for Non-Abelian Groups	5
A. The $q$ -SVP problem	5
B. Factoring integers over the real group	5
C. Period finding over $\mathbb{Z}$	5
D. Period finding over $\mathbb{Z}$	5
E. The period-finding problem and hidden subgroup problems	5
F. Computing the size of a group and the hidden subgroup	5
G. The period-finding problem and the hidden subgroup	5
VI. Non-Abelian Quantum Fourier Transforms	6
A. The Fourier transform over a non-Abelian group	6
B. Efficient quantum circuits	6

## Quantum Algorithms

Michèle Mosca

Institute for Quantum Computing and Dept. of Combinatorics & Optimization

University of Waterloo and St. Jerome's University

and Perimeter Institute for Theoretical Physics

[www.ipq.uwaterloo.ca/~mosca/](http://www.ipq.uwaterloo.ca/~mosca/)

## Article Outline

### Summary

1. Definition of the Subject and Its Importance
2. Introduction and Overview
3. The Early Quantum Algorithms
4. Factoring, Discrete Logarithms, and the Abelian Hidden Subgroup Problem
5. Algorithms based on Amplitude Amplification
6. Simulation of Quantum Mechanical Systems
7. Generalizations of the Abelian Hidden Subgroup Problem
8. Quantum Walk Algorithms
9. Adiabatic Algorithms
10. Topological Algorithms
11. Quantum algorithms for quantum tasks
12. Future Directions

## Algorithms for Quantum Computers

Josiah Smith and Michele Mosca

### 1 Introduction

Quantum computing is a new computational paradigm created by reformulating information and computation in a quantum mechanical framework [1, 2]. 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-

Authors' addresses:  
Josiah 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: [josiah.smith@utoronto.ca](mailto:josiah.smith@utoronto.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 MRC, NSERC, QuantumWorks, MITACS, CIFAR, CRC, DRI, and DTD-ARD  
e-mail: [michele.mosca@utoronto.ca](mailto:michele.mosca@utoronto.ca)

# Connecting abstract algorithms to devices

## IARPA

**BROAD AGENCY ANNOUNCEMENT: IARPA-BAA-10-02**

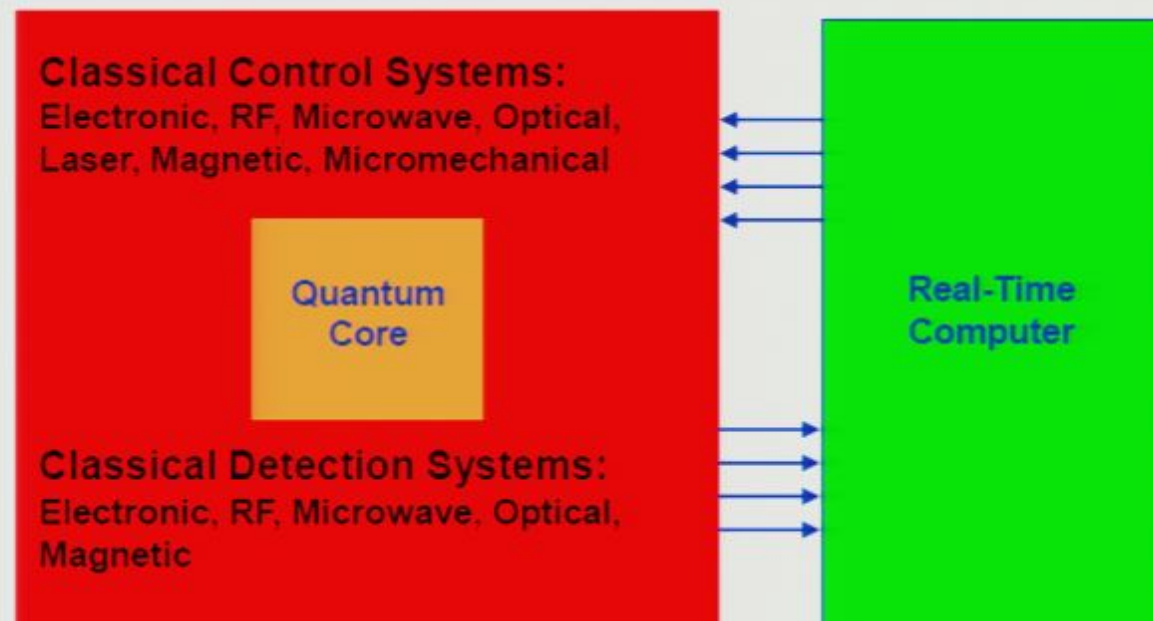
Quantum Computer Science (QCS) Program

“The QCS Program’s goal is to accurately estimate and significantly reduce the computational resources required to implement quantum algorithms on a realistic quantum computer.”



## *How is a quantum algorithm implemented?*

- ❑ Executing a quantum algorithm means performing a massive computer controlled quantum physics experiment.
- ❑ The full specification of how this experiment is to be carried out constitutes the implementation of a quantum algorithm.



**The quantum system core is expensive and fragile; therefore, we must minimize its number of qubits and operations.**



Are we ready to re-tool the existing crypto infrastructure?

# Are we ready to re-tool the existing crypto infrastructure?



Are we ready to re-tool the existing crypto infrastructure?

# Are we ready to re-tool the existing crypto infrastructure?

Correct answer: No.

A more informative answer:

# Are we ready to re-tool the existing crypto infrastructure?

Correct answer: No.

A more informative answer:

Alternatives to RSA (i.e. factoring-based cryptography) and ECC (i.e. discrete logarithm-based cryptography) are few and not as well scrutinized for security against classical or quantum attacks, or developed for practical deployability.

# Are we ready to re-tool the existing crypto infrastructure?

Correct answer: No.

A more informative answer:

Alternatives to RSA (i.e. factoring-based cryptography) and ECC (i.e. discrete logarithm-based cryptography) are few and not as well scrutinized for security against classical or quantum attacks, or developed for practical deployability.

Understanding the power of quantum algorithms, and their impact on computationally secure cryptography is an active area of research.

# Are we ready to re-tool the existing crypto infrastructure?

Correct answer: No.

A more informative answer:

Alternatives to RSA (i.e. factoring-based cryptography) and ECC (i.e. discrete logarithm-based cryptography) are few and not as well scrutinized for security against classical or quantum attacks, or developed for practical deployability.

Understanding the power of quantum algorithms, and their impact on computationally secure cryptography is an active area of research.



Fourth International Conference on Post-Quantum Cryptography



About the conference

**PQCrypto 2011, Nov 29 — Dec 2, Taipei**

# Quantum cryptographic tools

What about quantum communication?



# Quantum cryptographic tools

# Quantum cryptographic tools

What about quantum communication?

# Quantum cryptographic tools

What about quantum communication?

**Quantum communication can provide a new kind of cryptography that is “information theoretically” secure**

Typically in free-space or in fibre.

# Quantum cryptographic tools

What about quantum communication?

# Quantum cryptographic tools

What about quantum communication?

**Quantum communication can provide a new kind of cryptography that is “information theoretically” secure**

Typically in free-space or in fibre.

# Quantum cryptographic tools

What about quantum communication?

**Quantum communication can provide a new kind of cryptography that is “information theoretically” secure**

Typically in free-space or in fibre.

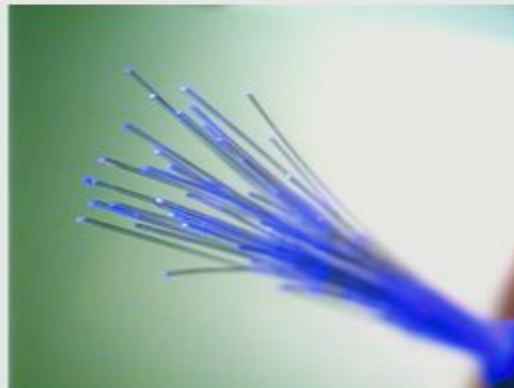


# Quantum cryptographic tools

What about quantum communication?

**Quantum communication can provide a new kind of cryptography that is “information theoretically” secure**

Typically in free-space or in fibre.

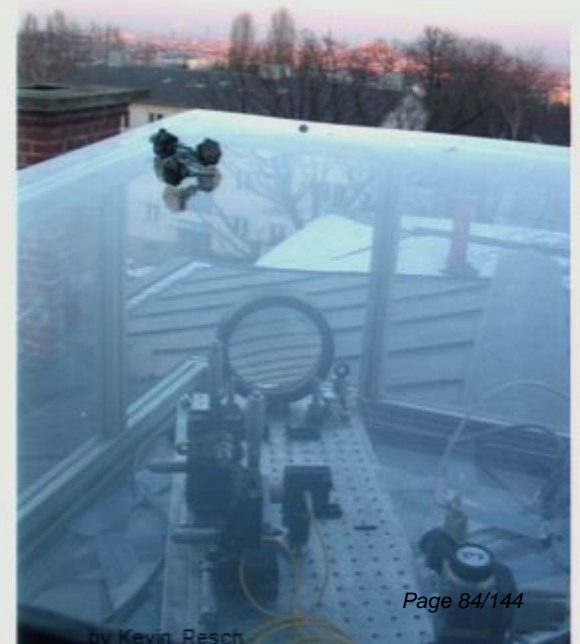
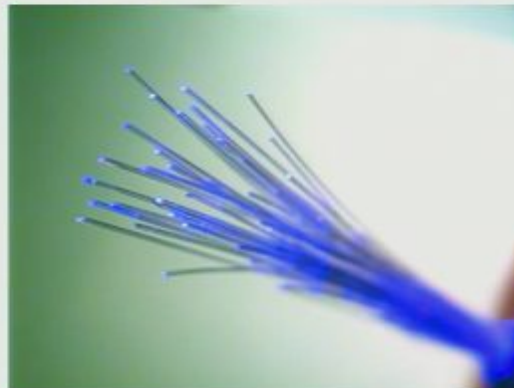


# Quantum cryptographic tools

What about quantum communication?

**Quantum communication can provide a new kind of cryptography that is “information theoretically” secure**

Typically in free-space or in fibre.



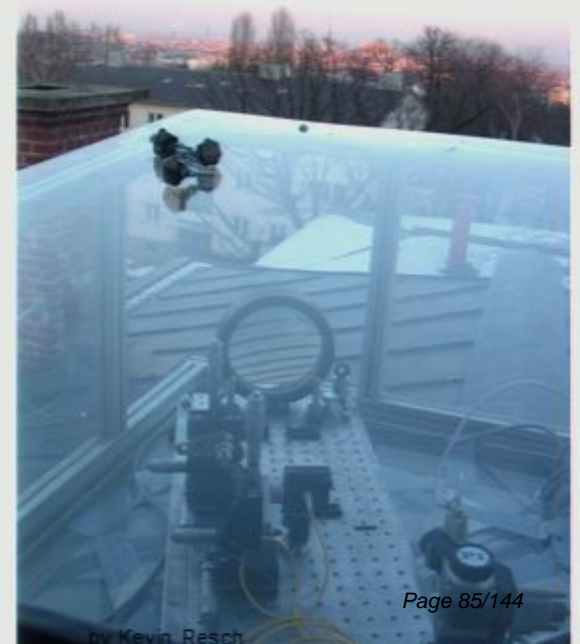
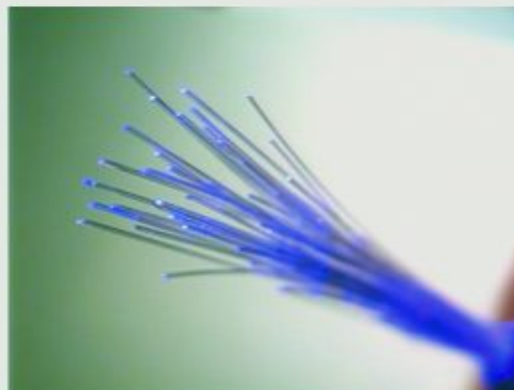
# Quantum cryptographic tools

What about quantum communication?

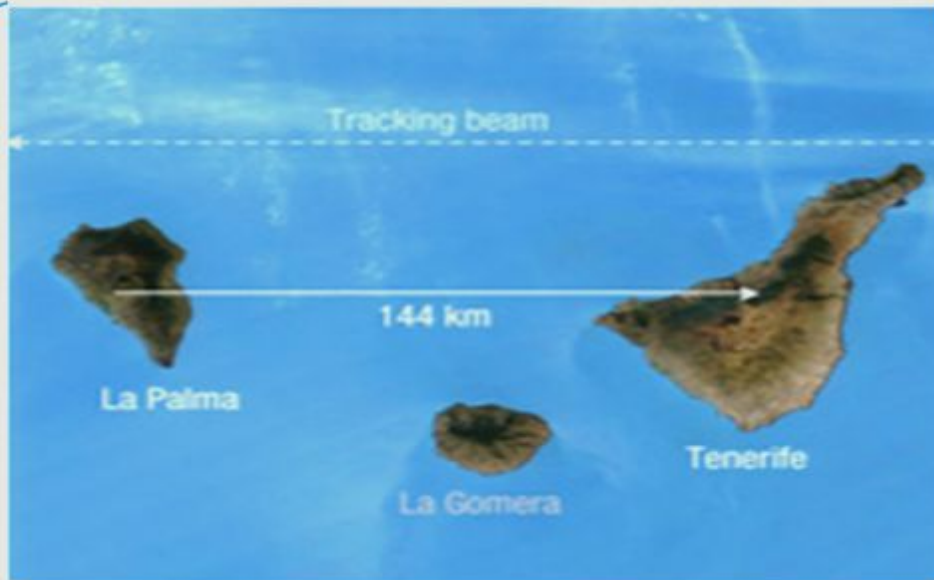
**Quantum communication can provide a new kind of cryptography that is “information theoretically” secure**

Typically in free-space or in fibre.


Will focus on QKD here, though many other quantum cryptography primitives are known (*ask Anne Broadbent*)







# Quantum Key Distribution Implementations around the world







 **mike.mosca** 



 € 6.41 - No subscription



 **Contacts**  **Recent** 



 Search



  Echo / Sound Test Service



  Home

  perimeter

  Adrienne Lo



  Andrew Childs

  Ashwin Nayak


  Austin Fowler



  Barry Sanders  
Imagination is more important.

  Douglas

 Add a contact  Create a group

 **Call phones**  
25,930,940 people online


 **Get group video calling**  
Share, celebrate and collaborate with up to 10 pe...

 Skype Home  Profile  Facebook

Learn how to use Skype

[View help videos](#)

News and alerts

[Show top contacts](#) 



Update your mood message

Top contacts



pbrancofonseca



Mark Reynolds



Austin Fowler



Richard Lazarus



Martin Roetteler



moscanelia



Ashwin Nayak



Lana



greenhatguy



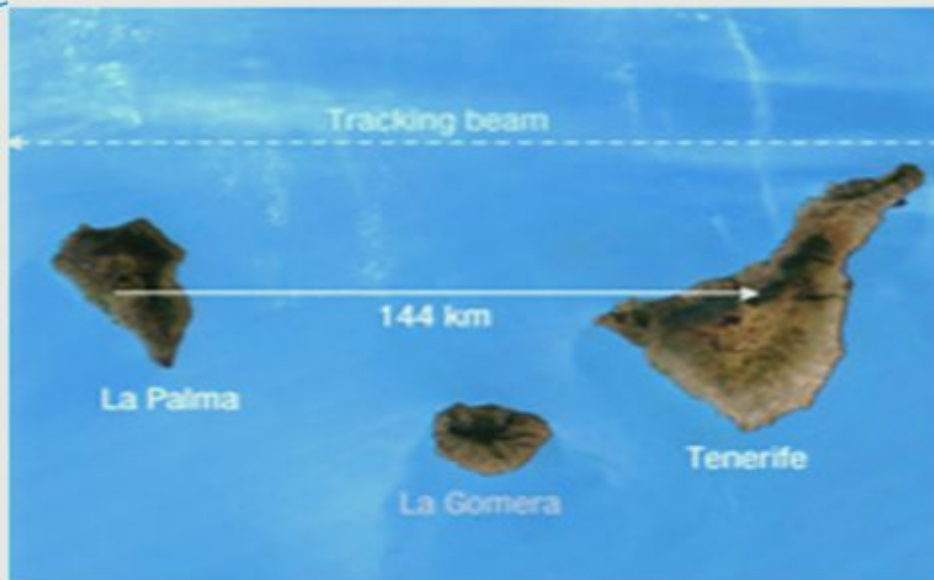
Lawrence Ioannou



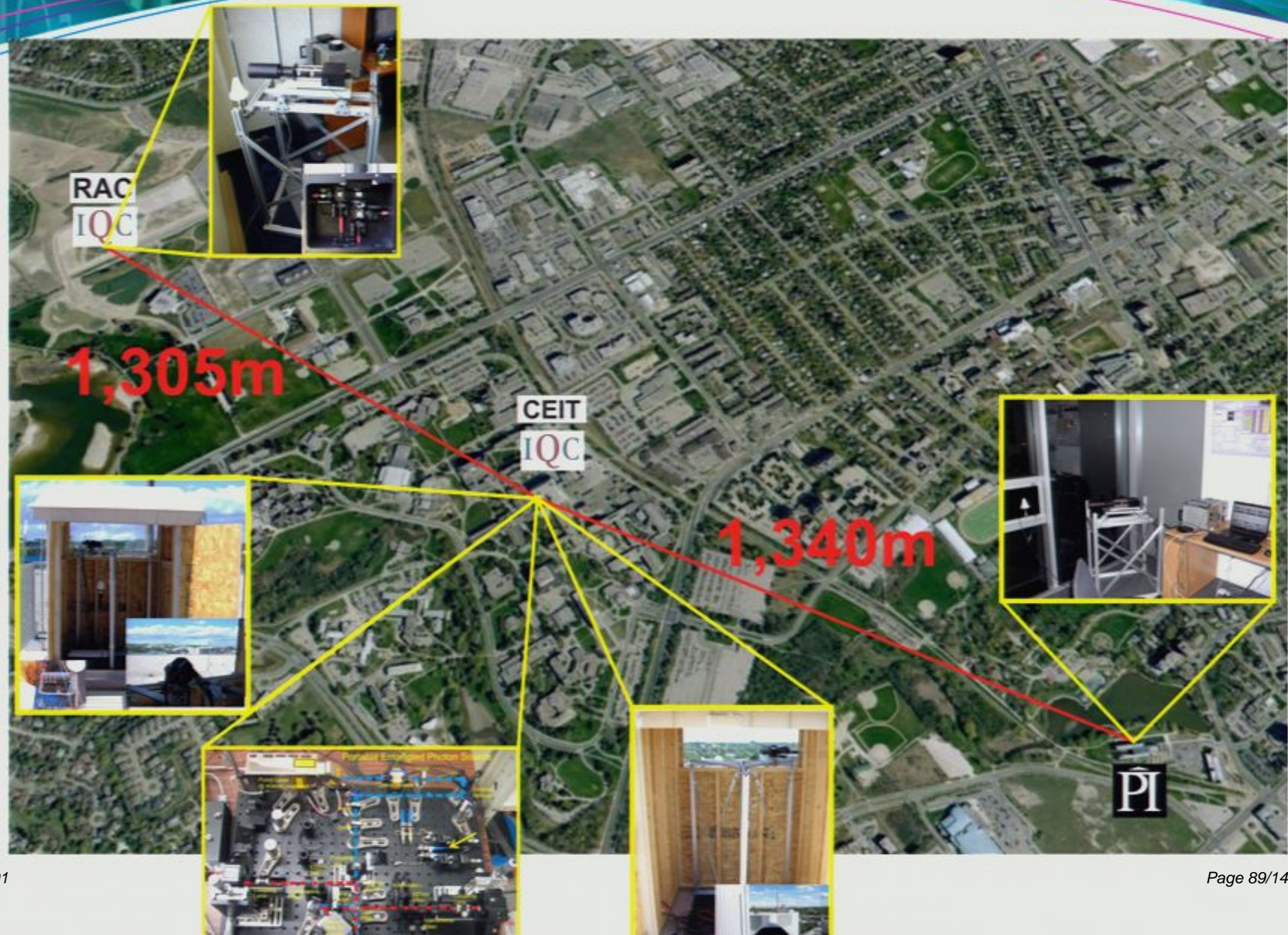
Password successfully changed

08/04/2011 9:03 PM

# Quantum Key Distribution Implementations around the world



# IQC QKD prototype



# Quantum communication networks

# Quantum communication networks

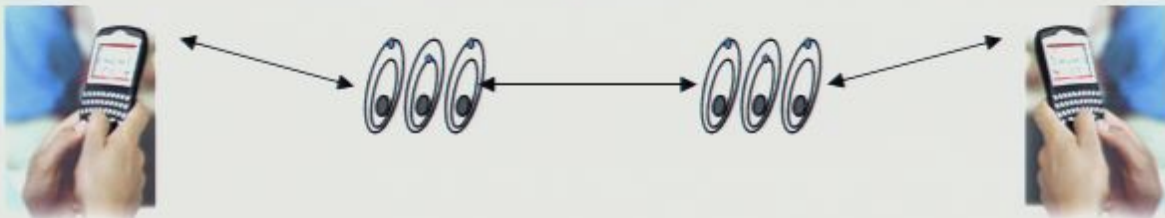
**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

*Quantum repeaters*

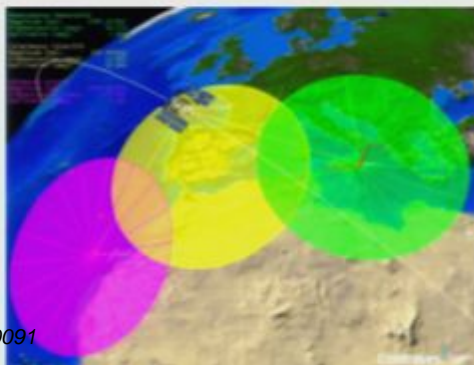
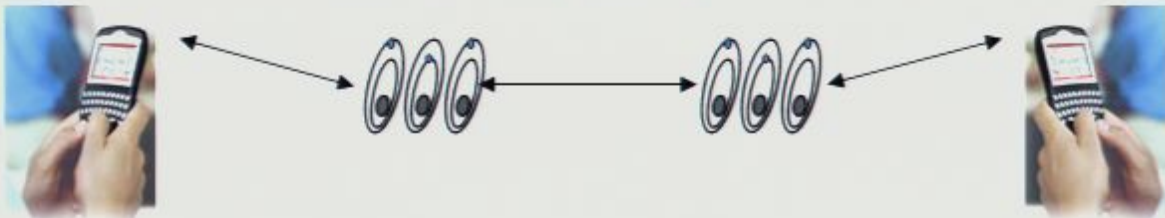


# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

*Quantum repeaters*



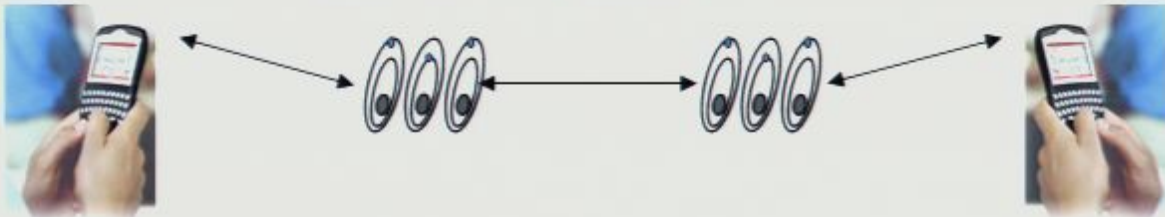
**Satellite-based quantum communications terminal employing state-of-the-art technology,**  
Pfennigbauer et al., JON 4, 549 (2005)

# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

*Quantum repeaters*

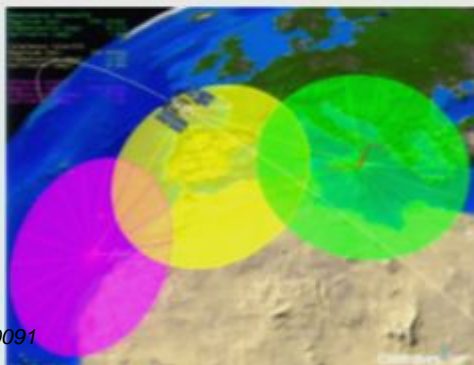
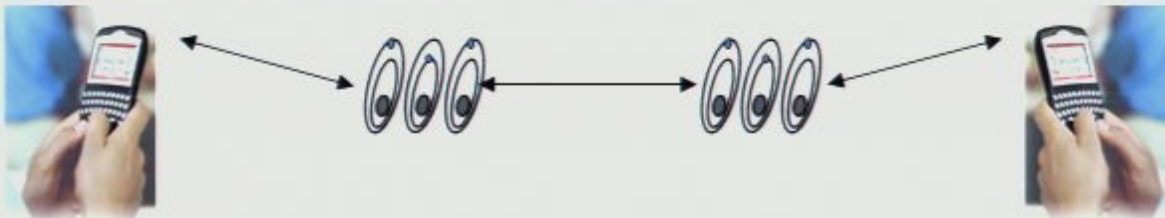


# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

*Quantum repeaters*



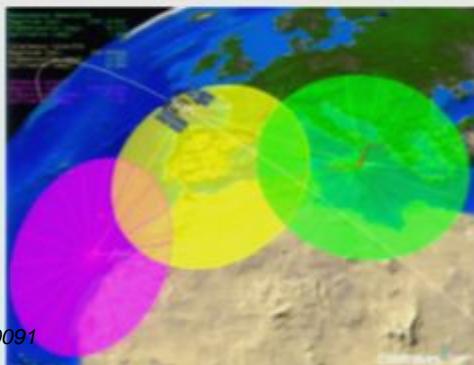
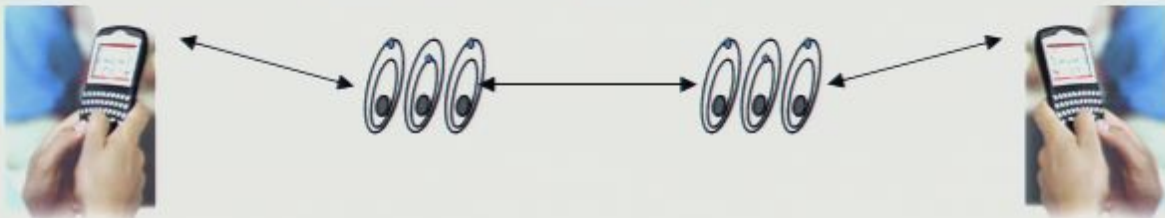
**Satellite-based quantum communications terminal employing state-of-the-art technology,**  
Pfennigbauer et al., JON 4, 549 (2005)

# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

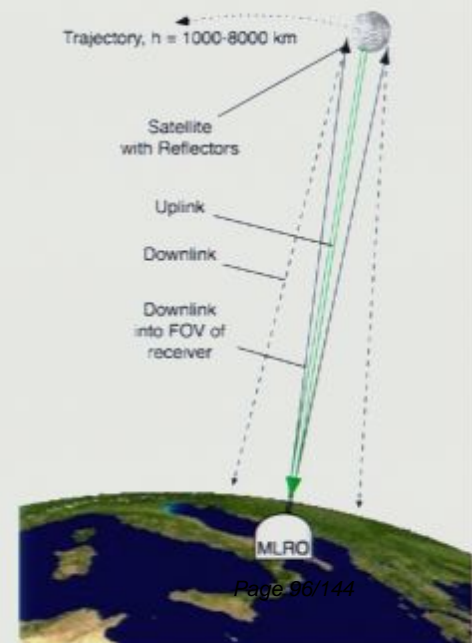
*Quantum repeaters*



**Satellite-based quantum communications terminal employing state-of-the-art technology,**  
Pfennigbauer et al., JON 4, 549 (2005)

**Experimental verification of the feasibility of a quantum channel between Space and Earth**

Villoresi et al. New Journal of Physics 10, 033038 (2008)

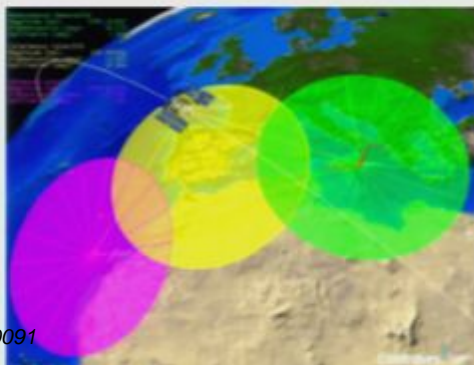
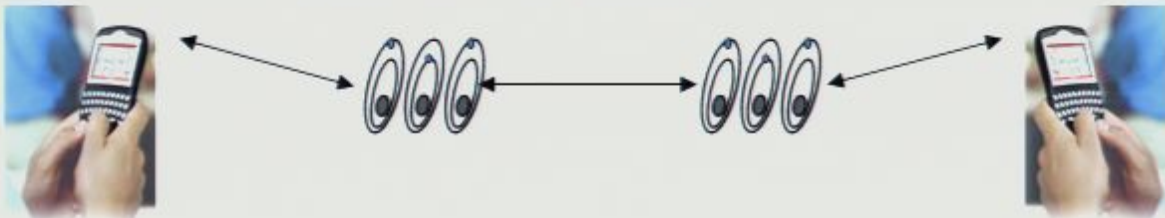


# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

*Quantum repeaters*



**Satellite-based quantum communications terminal employing state-of-the-art technology,**  
Pfennigbauer et al., JON 4, 549 (2005)

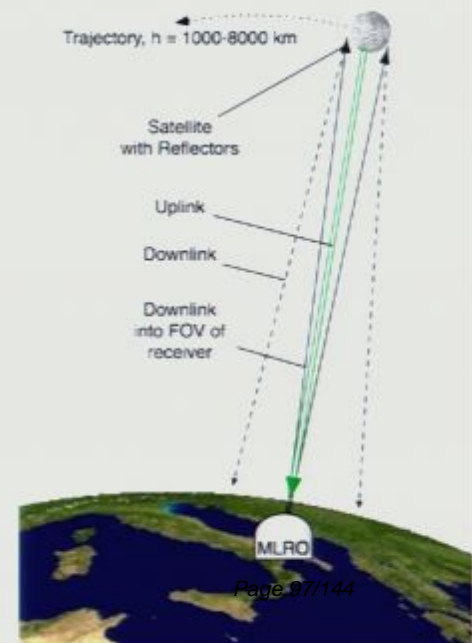
## Space-QUEST

Quantum Entanglement in Space Experiments

[www.quantum.at/quest](http://www.quantum.at/quest)

## Experimental verification of the feasibility of a quantum channel between Space and Earth

Villoresi et al. New Journal of Physics 10, 033038 (2008)



# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

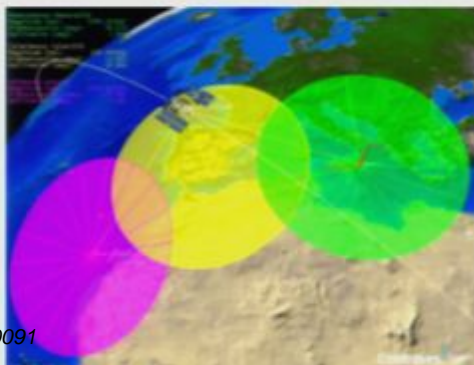
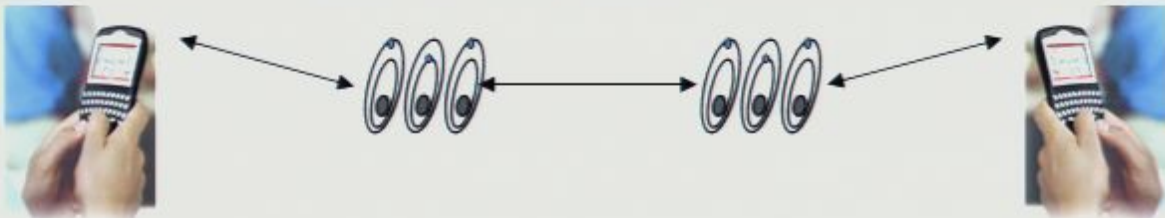
**“Security is a chain; it's as strong as the weakest link.** Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”

# Quantum communication networks

**At present, reliable quantum communication can be achieved along modest distances (approx. 100km)**

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

*Quantum repeaters*



**Satellite-based quantum communications terminal employing state-of-the-art technology,**  
Pfennigbauer et al., JON 4, 549 (2005)

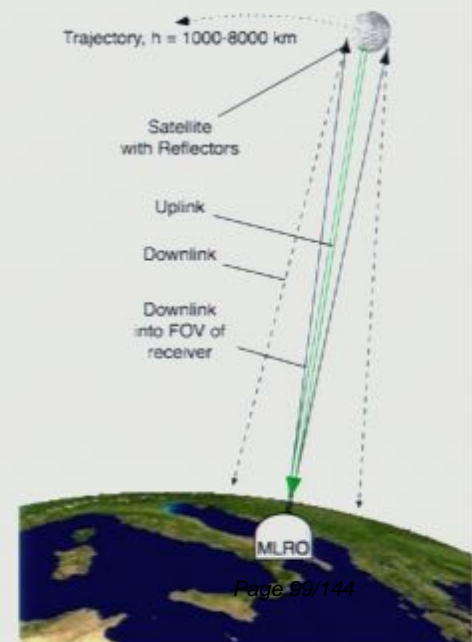
## Space-QUEST

Quantum Entanglement in Space Experiments

[www.quantum.at/quest](http://www.quantum.at/quest)

## Experimental verification of the feasibility of a quantum channel between Space and Earth

Villoresi et al. New Journal of Physics 10, 033038 (2008)



# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

**“Security is a chain; it's as strong as the weakest link.** Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”

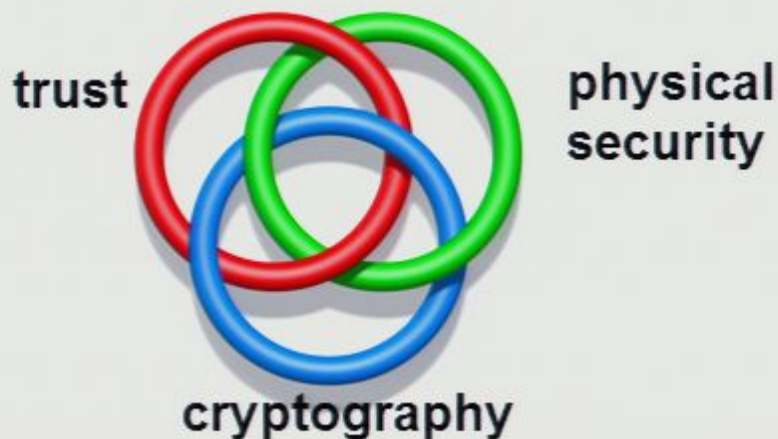
# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

**“Security is a chain; it's as strong as the weakest link.** Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”



# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

**“Security is a chain; it's as strong as the weakest link.** Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”

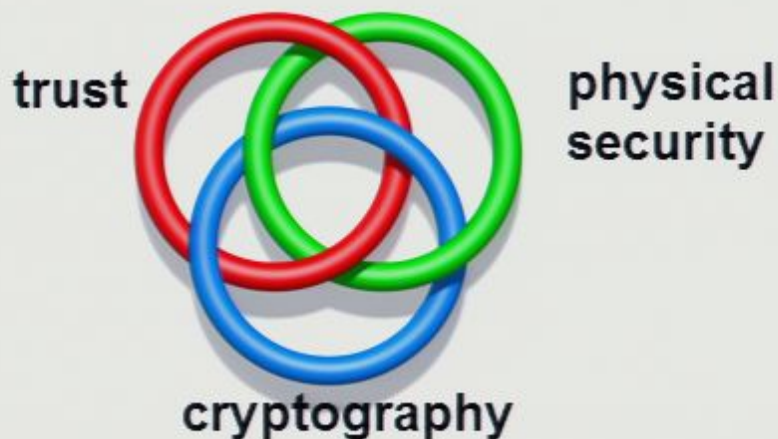
# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

**“Security is a chain; it's as strong as the weakest link.** Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”



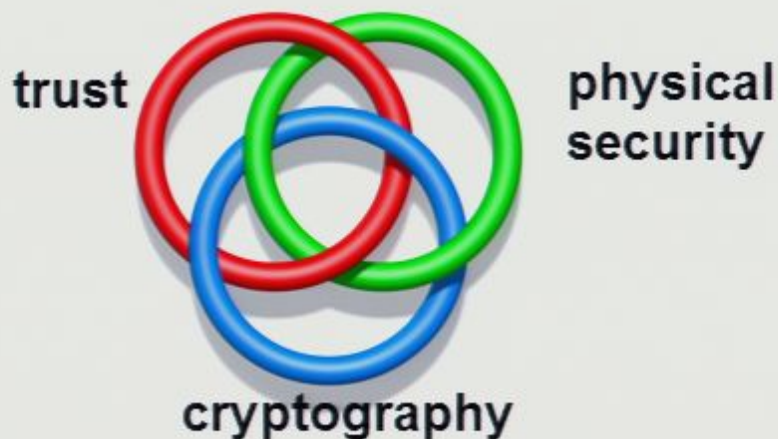
# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

**“Security is a chain; it's as strong as the weakest link. Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”**



## The Case for Quantum Key Distribution

Douglas Stebila<sup>1,2</sup>, Michele Mosca<sup>1,2,3</sup>, and Norbert Lütkenstrasse<sup>1,2,4</sup> \*

1. Institute for Quantum Computing, University of Waterloo

2. Dept. of Combinatorics & Optimization, University of Waterloo

3. Perimeter Institute for Theoretical Physics

4. Dept. of Physics & Astronomy, University of Waterloo  
Waterloo, Ontario, Canada

February 14, 2010

### Abstract

Quantum key distribution (QKD) promises secure key agreement by using quantum-mechanical systems. We argue that QKD will be an important part of future cryptographic infrastructure. It can provide long-term confidentiality for encrypted information without reliance on computational assumptions. Although QKD still requires authentication to prevent man-in-the-middle attacks, it can make use of either information-theoretically secure symmetric key authentication or computationally secure public key authentication: even when using public key authentication, we argue that QKD still offers stronger security than classical key agreement.

# Security of QKD implementations

There are attacks on commercial quantum systems, using properties of the physical devices used in the implementation.

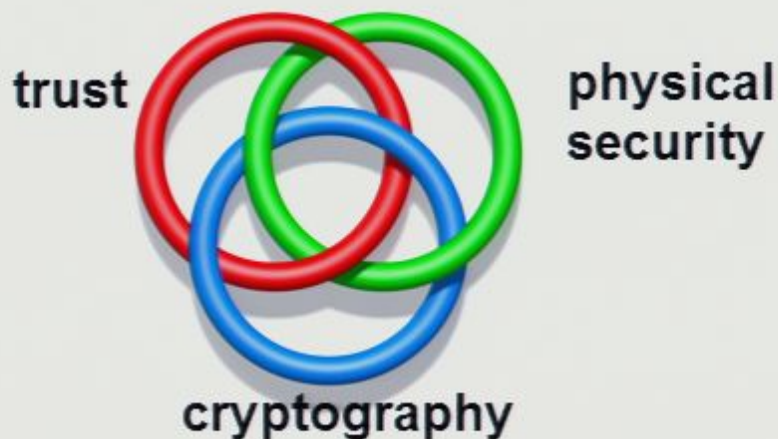
# Why use QKD in practice?

Schneier on Security

October 21, 2008

Quantum Cryptography

**“Security is a chain; it's as strong as the weakest link. Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. ... The real problems are elsewhere: computer security, network security, user interface and so on.”**



## The Case for Quantum Key Distribution

Douglas Stebila<sup>1,2</sup>, Michele Mosca<sup>1,2,3</sup>, and Norbert Lütkenstrasse<sup>1,2,4</sup> \*

1. Institute for Quantum Computing, University of Waterloo

2. Dept. of Combinatorics & Optimization, University of Waterloo

3. Perimeter Institute for Theoretical Physics

4. Dept. of Physics & Astronomy, University of Waterloo  
Waterloo, Ontario, Canada

February 14, 2010

### Abstract

Quantum key distribution (QKD) promises secure key agreement by using quantum-mechanical systems. We argue that QKD will be an important part of future cryptographic infrastructure. It can provide long-term confidentiality for encrypted information without reliance on computational assumptions. Although QKD still requires authentication to prevent man-in-the-middle attacks, it can make use of either information-theoretically secure symmetric key authentication or computationally secure public key authentication; even when using public key authentication, we argue that QKD still offers stronger security than classical key agreement.

# Security of QKD implementations

There are attacks on commercial quantum systems, using properties of the physical devices used in the implementation.

Recent device independent proposals for QKD try to avoid these situations.

# Security of QKD implementations

There are attacks on commercial quantum systems, using properties of the physical devices used in the implementation.

Recent device independent proposals for QKD try to avoid these situations.

NATURE PHOTONICS | LETTER

## Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

[Affiliations](#) · [Contributions](#) · [Corresponding author](#)

Nature Photonics 4, 686–689 (2010) | doi:10.1038/nphoton.2010.214

Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

PRL 105, 070501 (2010)

PHYSICAL REVIEW LETTERS

week ending  
13 AUGUST 2010

## Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier

Nicolas Gisin,<sup>1</sup> Stefano Pironio,<sup>1,2</sup> and Nicolas Sangouard<sup>1</sup>

<sup>1</sup>Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

<sup>2</sup>Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium

(Received 22 March 2010; revised manuscript received 13 July 2010; published 12 August 2010)

# Security of QKD implementations

There are attacks on commercial quantum systems, using properties of the physical devices used in the implementation.

Recent device independent proposals for QKD try to avoid these situations.

NATURE PHOTONICS | LETTER

## Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Affiliations · Contributions · Corresponding author

Nature Photonics 4, 686–689 (2010) | doi:10.1038/nphoton.2010.214

Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

PRL 105, 070501 (2010)

PHYSICAL REVIEW LETTERS

week ending  
13 AUGUST 2010

## Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier

Nicolas Gisin,<sup>1</sup> Stefano Pironio,<sup>1,2</sup> and Nicolas Sangouard<sup>1</sup>

<sup>1</sup>Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

<sup>2</sup>Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium

(Received 22 March 2010; revised manuscript received 13 July 2010; published 12 August 2010)

Directly addressing physical security/side-channel issues is an important step in the maturation of the technology.

# Commercial QKD products and research

MagiQ QPN™ Security Gateway

Uncompromising VPN Security™

"Quantum Cryptography: when your link has to be very, very secure."

By Bill Schweber, EDN, 12/6/05



id Quantique

A Quantum Leap For Cryptography



NEC

Empowered by Innovation

Princeton Lightwave



World Class Standards

IBM

**UQCC 2010**  
Updating Quantum Cryptography and Communications 2010  
October 18-20, 2010, ANA INTERCONTINENTAL TOKYO  
"See & touch the quantum inspired future"  
Tokyo QKD Network

National Institute of Standards and Technology

NIST

Telcordia

# Security of QKD implementations

There are attacks on commercial quantum systems, using properties of the physical devices used in the implementation.

Recent device independent proposals for QKD try to avoid these situations.

NATURE PHOTONICS | LETTER

## Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Affiliations · Contributions · Corresponding author

Nature Photonics 4, 686–689 (2010) | doi:10.1038/nphoton.2010.214

Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

PRL 105, 070501 (2010)

PHYSICAL REVIEW LETTERS

week ending  
13 AUGUST 2010

## Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier

Nicolas Gisin,<sup>1</sup> Stefano Pironio,<sup>1,2</sup> and Nicolas Sangouard<sup>1</sup>

<sup>1</sup>Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

<sup>2</sup>Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium

(Received 22 March 2010; revised manuscript received 13 July 2010; published 12 August 2010)

Directly addressing physical security/side-channel issues is an important step in the maturation of the technology.

# Commercial QKD products and research

MagiQ QPN™ Security Gateway

Uncompromising VPN Security™

"Quantum Cryptography: when your link has to be very, very secure."

By Bill Schweber, EDN, 12/6/05



id Quantique

A Quantum Leap For Cryptography



NEC

Empowered by Innovation

Princeton  
Lightwave

UQCC 2010  
Updating Quantum Cryptography and Communications 2010  
October 18-20, 2010, ANA INTERCONTINENTAL TOKYO  
"See & touch the quantum inspired future"  
Tokyo QKD Network



World Class Standards

IBM

National Institute of  
Standards and Technology

NIST

Telcordia

# Further information...

Deutsche Physikalische Gesellschaft  DPG | IOP Institute of Physics

[New Journal of Physics Volume 11 April 2009 Create an alertRSS this journal](#)

N Lütkenhaus and A J Shields 2009 *New J. Phys.* **11** 045005 doi: [10.1088/1367-2630/11/4/045005](https://doi.org/10.1088/1367-2630/11/4/045005)

## Focus on Quantum Cryptography: Theory and Practice

[Focus on Quantum Crvptography: Theory and Practice](#)

N Lütkenhaus<sup>1</sup> and A J Shields<sup>2</sup>

<sup>1</sup> Institute for Quantum Computing, Department of Physics & Astronomy, University of Waterloo, Canada

<sup>2</sup> Quantum Information Group, Toshiba Research Europe, Cambridge, UK

# Quantum Sensing

Quantum information processing will transform computation, communication and *sensing* technologies. e.g.

Longer-Baseline Telescopes Using Quantum Repeaters

Daniel Gottesman<sup>\*1</sup>, Thomas Jennewein<sup>†2</sup>, and Sarah Croke<sup>‡1</sup>

<sup>1</sup> Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

<sup>2</sup> Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada

The two primary goals for a telescope are sensitivity and angular resolution. Interferometry among telescope arrays has become a standard technique in astronomy, allowing greater resolving power than would be available to a single telescope. In today's IR and optical interferometric arrays [1, 2], photons arriving at different telescopes must be physically brought together for the interference measurement, limiting baselines to a few hundred meters at most because of phase fluctuations and photon loss in the transmission. Improved resolution would, if accompanied by adequate sensitivity, have many scientific applications, such as detailed observational studies of active galactic nuclei, more sensitive parallax measurements to improve our knowledge of stellar distances, or imaging of extra-solar planets. The field of quantum

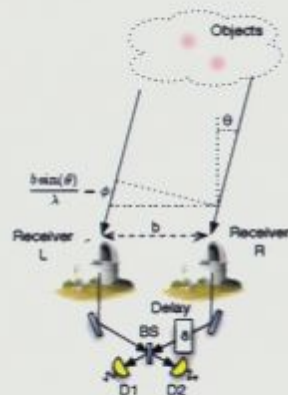
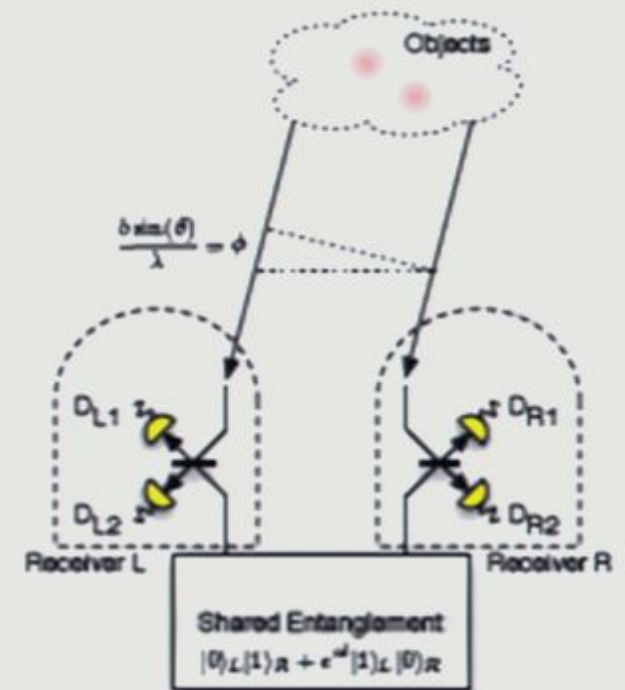


Figure 1: Basic set-up of a direct-detection interferometer



# Further information...

(see Jeffery, Holloway talks)

Deutsche Physikalische Gesellschaft  DPG | IOP Institute of Physics

[New Journal of Physics Volume 11 April 2009 Create an alertRSS this journal](#)

N Lütkenhaus and A J Shields 2009 *New J. Phys.* **11** 045005 doi: [10.1088/1367-2630/11/4/045005](https://doi.org/10.1088/1367-2630/11/4/045005)

## Focus on Quantum Cryptography: Theory and Practice

[Focus on Quantum Crvptography: Theory and Practice](#)

N Lütkenhaus<sup>1</sup> and A J Shields<sup>2</sup>

<sup>1</sup> Institute for Quantum Computing, Department of Physics & Astronomy, University of Waterloo, Canada

<sup>2</sup> Quantum Information Group, Toshiba Research Europe, Cambridge, UK

# Quantum Sensing

Quantum information processing will transform computation, communication and *sensing* technologies. e.g.

Longer-Baseline Telescopes Using Quantum Repeaters

Daniel Gottesman<sup>\*1</sup>, Thomas Jennewein<sup>†2</sup>, and Sarah Croke<sup>‡1</sup>

<sup>1</sup> Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

<sup>2</sup> Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada

The two primary goals for a telescope are sensitivity and angular resolution. Interferometry among telescope arrays has become a standard technique in astronomy, allowing greater resolving power than would be available to a single telescope. In today's IR and optical interferometric arrays [1, 2], photons arriving at different telescopes must be physically brought together for the interference measurement, limiting baselines to a few hundred meters at most because of phase fluctuations and photon loss in the transmission. Improved resolution would, if accompanied by adequate sensitivity, have many scientific applications, such as detailed observational studies of active galactic nuclei, more sensitive parallax measurements to improve our knowledge of stellar distances, or imaging of extra-solar planets. The field of quantum

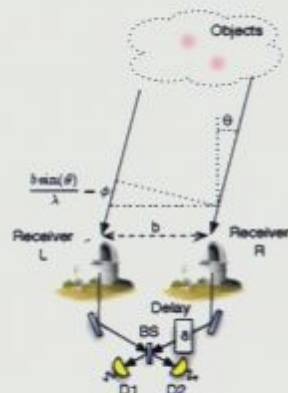
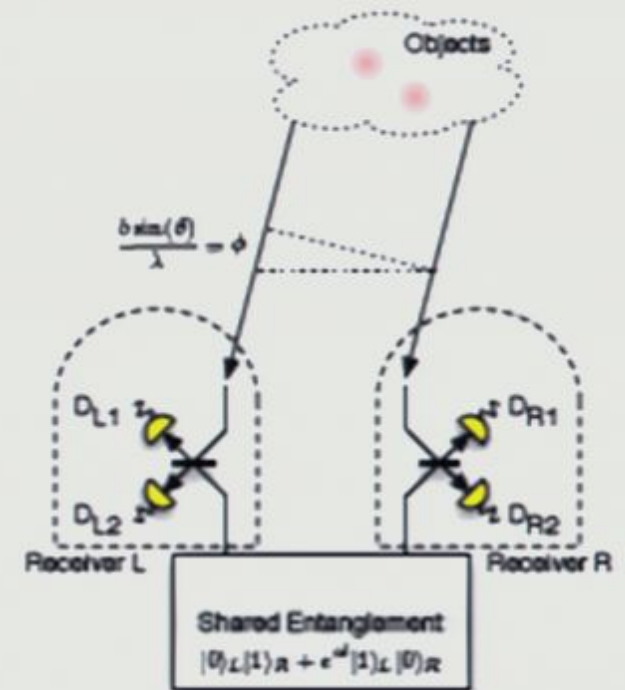


Figure 1: Basic set-up of a direct-detection interferometer



# Quantum Information in Foundational Physics

## Black holes as mirrors: quantum information in random subsystems

Patrick Hayden

*School of Computer Science, McGill University, Montreal, Quebec, H3A 2A7, Canada*

John Preskill

*Institute for Quantum Information, California Institute of Technology, Pasadena CA 91125, USA*

### Abstract

We study information retrieval from evaporating black holes, assuming that the internal dynamics of a black hole is unitary and rapidly mixing, and assuming that the retriever has unlimited control over the emitted Hawking radiation. If the evaporation of the black hole has already proceeded past the ‘half-way’ point, where half of the initial entropy has been radiated away, then additional quantum information deposited in the black hole is revealed in the Hawking radiation very rapidly. Information deposited prior to the half-way point remains concealed until the half-way point, and then emerges quickly. These conclusions hold because typical local quantum circuits are efficient encoders for quantum error-correcting codes that nearly achieve the capacity of the quantum erasure channel. Our estimate of a black hole’s information retention time, based on speculative dynamical assumptions, is just barely compatible with the black hole complementarity hypothesis.

## Simulating quantum effects of cosmological expansion using a static ion trap

Nicola C. Menicucci,<sup>1</sup> S. Jay Olson,<sup>2</sup> and Gerard J. Milburn<sup>2</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada*

<sup>2</sup>*Centre for Quantum Computer Technology, School of Mathematics and Physics,  
The University of Queensland, St. Lucia, QLD, 4072, Australia*

(Date: August 2, 2010)

We propose a new experimental setup that uses ions in the collective ground state of a static trap for studying the analog of quantum-field effects in cosmological spacetimes, including the Gibbons-Hawking effect for a single detector in de Sitter spacetime, as well as the possibility of modeling inflationary structure formation and the entanglement signature of de Sitter spacetime. To date, proposals for using trapped ions in analog gravity experiments have simulated the effect of gravity on the field modes by directly manipulating the ions’ motion. In contrast, by associating laboratory time with conformal time in the simulated universe, we can encode the full effect of curvature in the modulation of the laser used to couple the ions’ vibrational motion and electronic states. This model simplifies the experimental requirements for modeling the analog of an expanding universe using trapped ions and enlarges the validity of the ion-trap analogy to a wide range of interesting cases.

PACS numbers: 03.65.-w, 04.62.+g, 37.10.Ty, 42.50.Cz

## Some Calculable Contributions to Holographic Entanglement Entropy

Ling-Yan Hung, Robert C. Myers and Michael Smolkin

*Perimeter Institute for Theoretical Physics,*

*31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*

**ABSTRACT:** Using the AdS/CFT correspondence, we examine entanglement entropy for a boundary theory deformed by a relevant operator and establish two results. The first is that if there is a contribution which is logarithmic in the UV cut-off, then the coefficient of this term is independent of the state of the boundary theory. In fact, the same is true of all of the coefficients of contributions which diverge as some power of the UV cut-off. Secondly, we show that the relevant deformation introduces new logarithmic contributions to the entanglement entropy. The form of some of these new contributions is similar to that found recently in an investigation of entanglement entropy in a free massive scalar field theory [1].

## Background independent condensed matter models for quantum gravity

Allencia Hamma<sup>1</sup> and Fotis Markopoulou<sup>1,2,4</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, 31 Caroline St. N. N2L 2Y5 Waterloo ON, Canada*

<sup>2</sup>*Department of Physics, University of Waterloo, Waterloo, Ontario N2L 2G1, Canada*

<sup>3</sup>*Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut), Am Mühlenberg 1, D-14476 Golm, Germany*

<sup>4</sup>*Simon Stevin Institute, 1000 Hyde Park Road, 07508 Sussex Pa, USA*

A number of recent proposals for a quantum theory of gravity are based on the idea that spacetime geometry and gravity are derivative concepts and only apply at an approximate level. There are two fundamental challenges to any such approach. At the conceptual level, there is a clash between the ‘‘fuzziness’’ of general relativity and emergence. Second, the lack of a fundamental quantum makes difficult the straightforward application of well-known methods of statistical physics to the problem. We propose instead a study of such problems using spin systems based on evaluation of quantum networks with no a priori geometric notions as models for emergent geometry and gravity.

In this article we review two such models. The first is a model of emergent (flat) space and matter and we show how to use methods from quantum information theory to derive features such as speed of light from a non-geometric quantum system. The second model exhibits interacting matter and geometry, with the geometry defined by the behavior of matter. This model has primitive notions of gravitational attraction which we illustrate with a toy black hole, and exhibits entanglement between matter and geometry and discretization of the quantum geometry.

PACS numbers:

Niv:1105.6055v1 [hep-th] 30 May 2011

26 Nov 2010

25v2 [hep-th] 21 Sep 2007

-ph] 2 Aug 2010

# Quantum Sensing

Quantum information processing will transform computation, communication and *sensing* technologies. e.g.

Longer-Baseline Telescopes Using Quantum Repeaters

Daniel Gottesman<sup>\*1</sup>, Thomas Jennewein<sup>†2</sup>, and Sarah Croke<sup>‡1</sup>

<sup>1</sup> Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

<sup>2</sup> Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada

The two primary goals for a telescope are sensitivity and angular resolution. Interferometry among telescope arrays has become a standard technique in astronomy, allowing greater resolving power than would be available to a single telescope. In today's IR and optical interferometric arrays [1, 2], photons arriving at different telescopes must be physically brought together for the interference measurement, limiting baselines to a few hundred meters at most because of phase fluctuations and photon loss in the transmission. Improved resolution would, if accompanied by adequate sensitivity, have many scientific applications, such as detailed observational studies of active galactic nuclei, more sensitive parallax measurements to improve our knowledge of stellar distances, or imaging of extra-solar planets. The field of quantum

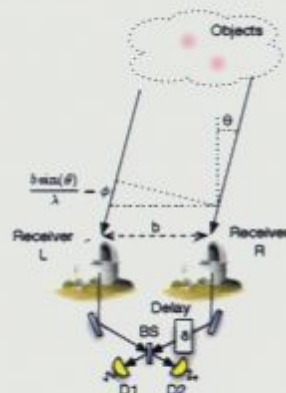
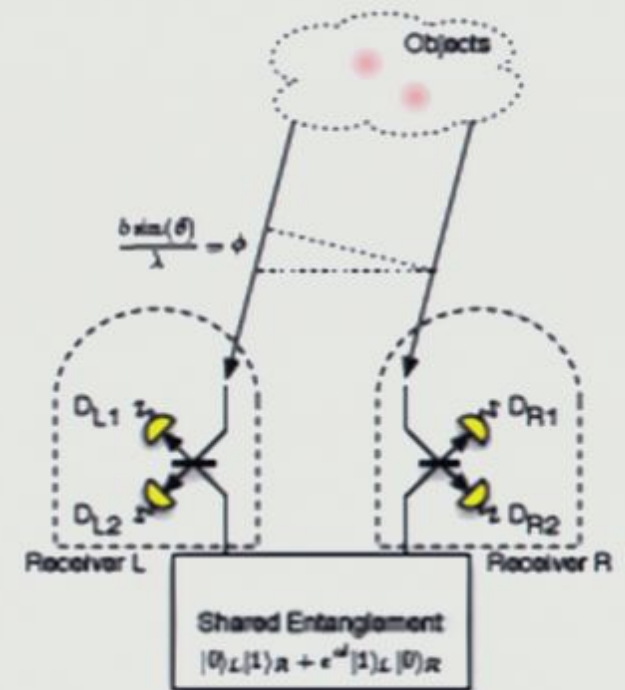


Figure 1: Basic set-up of a direct detection interferometer



# Quantum Information in Foundational Physics

## Black holes as mirrors: quantum information in random subsystems

Patrick Hayden

*School of Computer Science, McGill University, Montreal, Quebec, H3A 2A7, Canada*

John Preskill

*Institute for Quantum Information, California Institute of Technology, Pasadena CA 91125, USA*

### Abstract

We study information retrieval from evaporating black holes, assuming that the internal dynamics of a black hole is unitary and rapidly mixing, and assuming that the retriever has unlimited control over the emitted Hawking radiation. If the evaporation of the black hole has already proceeded past the ‘half-way’ point, where half of the initial entropy has been radiated away, then additional quantum information deposited in the black hole is revealed in the Hawking radiation very rapidly. Information deposited prior to the half-way point remains concealed until the half-way point, and then emerges quickly. These conclusions hold because typical local quantum circuits are efficient encoders for quantum error-correcting codes that nearly achieve the capacity of the quantum erasure channel. Our estimate of a black hole’s information retention time, based on speculative dynamical assumptions, is just barely compatible with the black hole complementarity hypothesis.

## Simulating quantum effects of cosmological expansion using a static ion trap

Nicola C. Menicucci,<sup>1</sup> S. Jay Olson,<sup>2</sup> and Gerard J. Milburn<sup>2</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada*

<sup>2</sup>*Centre for Quantum Computer Technology, School of Mathematics and Physics,  
The University of Queensland, St Lucia, QLD, 4072, Australia*

(Date: August 2, 2010)

We propose a new experimental setup that uses ions in the collective ground state of a static trap for studying the analog of quantum-field effects in cosmological spacetimes, including the Gibbons-Hawking effect for a single detector in de Sitter spacetime, as well as the possibility of modeling inflationary structure formation and the entanglement signature of de Sitter spacetime. To date, proposals for using trapped ions in analog gravity experiments have simulated the effect of gravity on the field modes by directly manipulating the ions’ motion. In contrast, by associating laboratory time with conformal time in the simulated universe, we can encode the full effect of curvature in the modulation of the laser used to couple the ions’ vibrational motion and electronic states. This model simplifies the experimental requirements for modeling the analog of an expanding universe using trapped ions and enlarges the validity of the ion-trap analogy to a wide range of interesting cases.

PACS numbers: 03.55.-w, 04.62.+v, 37.10.Ty, 42.50.Cx

## Some Calculable Contributions to Holographic Entanglement Entropy

Ling-Yan Hung, Robert C. Myers and Michael Smolkin

*Perimeter Institute for Theoretical Physics,*

*31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*

**ABSTRACT:** Using the AdS/CFT correspondence, we examine entanglement entropy for a boundary theory deformed by a relevant operator and establish two results. The first is that if there is a contribution which is logarithmic in the UV cut-off, then the coefficient of this term is independent of the state of the boundary theory. In fact, the same is true of all of the coefficients of contributions which diverge as some power of the UV cut-off. Secondly, we show that the relevant deformation introduces new logarithmic contributions to the entanglement entropy. The form of some of these new contributions is similar to that found recently in an investigation of entanglement entropy in a free massive scalar field theory [1].

## Background independent condensed matter models for quantum gravity

Allodia Hamma<sup>1</sup> and Fotis Markopoulou<sup>1,2,4</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, 31 Caroline St. N. N2L 2Y5, Waterloo (ON, Canada)*

<sup>2</sup>*Department of Physics, University of Waterloo, Waterloo, Ontario N2L 2G1, Canada*

<sup>3</sup>*Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut), Am Mühlenberg 1, D-14476 Golm, Germany*

<sup>4</sup>*Santa Fe Institute, 1099 Hyde Park Road, SF 808 Santa Fe, USA*

A number of recent proposals for a quantum theory of gravity are based on the idea that spacetime geometry and gravity are derivative concepts and only apply at an approximate level. There are two fundamental challenges to any such approach. At the conceptual level, there is a clash between the ‘‘bottomness’’ of general relativity and emergence. Second, the lack of a fundamental quantum makes difficult the straightforward application of well-known methods of statistical physics to the problem. We recently initiated a study of such problems using spin systems based on evaluation of quantum networks with no a priori geometric notions as models for emergent geometry and gravity.

In this article we review two such models. The first is a model of emergent (flat) space and matter and we show how to use methods from quantum information theory to derive features such as speed of light from a non-geometric quantum system. The second model exhibits interacting matter and geometry, with the geometry defined by the behavior of matter. This model has primitive notions of gravitational attraction which we illustrate with a toy black hole, and exhibits entanglement between matter and geometry and thermalization of the quantum geometry.

PACS numbers:

Niv:1105.6055v1 [hep-th] 30 May 2011

26 Nov 2010

25v2 [hep-th] 21 Sep 2007

-ph] 2 Aug 2010

# Quantum Sensing

Quantum information processing will transform computation, communication and *sensing* technologies. e.g.

Longer-Baseline Telescopes Using Quantum Repeaters

Daniel Gottesman<sup>\*1</sup>, Thomas Jennewein<sup>†2</sup>, and Sarah Croke<sup>‡1</sup>

<sup>1</sup> Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

<sup>2</sup> Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada

The two primary goals for a telescope are sensitivity and angular resolution. Interferometry among telescope arrays has become a standard technique in astronomy, allowing greater resolving power than would be available to a single telescope. In today's IR and optical interferometric arrays [1, 2], photons arriving at different telescopes must be physically brought together for the interference measurement, limiting baselines to a few hundred meters at most because of phase fluctuations and photon loss in the transmission. Improved resolution would, if accompanied by adequate sensitivity, have many scientific applications, such as detailed observational studies of active galactic nuclei, more sensitive parallax measurements to improve our knowledge of stellar distances, or imaging of extra-solar planets. The field of quantum

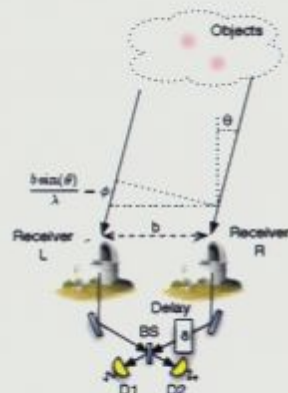
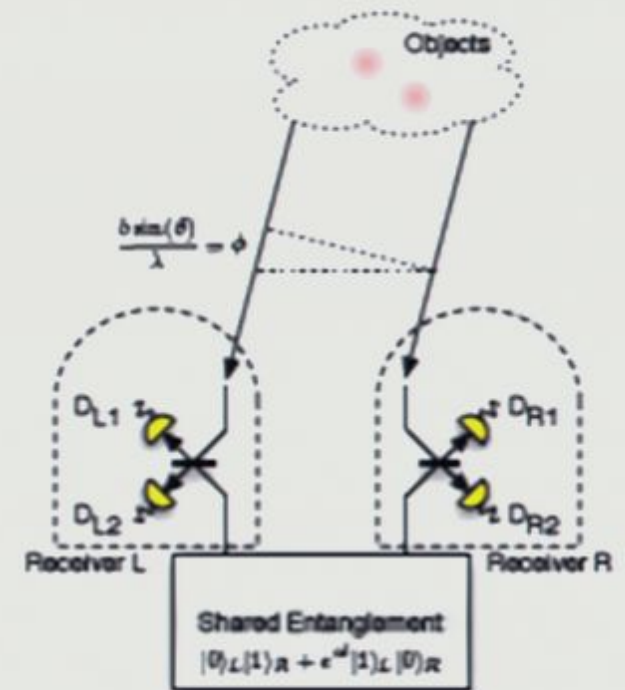


Figure 1: Basic set-up of a direct detection interferometer



# Quantum Information in Foundational Physics

## Black holes as mirrors: quantum information in random subsystems

Patrick Hayden

*School of Computer Science, McGill University, Montreal, Quebec, H3A 2A7, Canada*

John Preskill

*Institute for Quantum Information, California Institute of Technology, Pasadena CA 91125, USA*

### Abstract

We study information retrieval from evaporating black holes, assuming that the internal dynamics of a black hole is unitary and rapidly mixing, and assuming that the retriever has unlimited control over the emitted Hawking radiation. If the evaporation of the black hole has already proceeded past the ‘half-way’ point, where half of the initial entropy has been radiated away, then additional quantum information deposited in the black hole is revealed in the Hawking radiation very rapidly. Information deposited prior to the half-way point remains concealed until the half-way point, and then emerges quickly. These conclusions hold because typical local quantum circuits are efficient encoders for quantum error-correcting codes that nearly achieve the capacity of the quantum erasure channel. Our estimate of a black hole’s information retention time, based on speculative dynamical assumptions, is just barely compatible with the black hole complementarity hypothesis.

## Simulating quantum effects of cosmological expansion using a static ion trap

Nicolas C. Menicucci,<sup>1</sup> S. Jay Olson,<sup>2</sup> and Gerard J. Milburn<sup>2</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada*

<sup>2</sup>*Centre for Quantum Computer Technology, School of Mathematics and Physics,  
The University of Queensland, St. Lucia, QLD, 4072, Australia*

(Dated: August 2, 2010)

We propose a new experimental setup that uses ions in the collective ground state of a static trap for studying the analog of quantum-field effects in cosmological spacetimes, including the Gibbons-Hawking effect for a single detector in de Sitter spacetime, as well as the possibility of modeling inflationary structure formation and the entanglement signature of de Sitter spacetime. To date, proposals for using trapped ions in analog gravity experiments have simulated the effect of gravity on the field modes by directly manipulating the ions’ motion. In contrast, by associating laboratory time with conformal time in the simulated universe, we can encode the full effect of curvature in the modulation of the laser used to couple the ions’ vibrational motion and electronic states. This model simplifies the experimental requirements for modeling the analog of an expanding universe using trapped ions and enlarges the validity of the ion-trap analogy to a wide range of interesting cases.

PACS numbers: 03.65.-w, 04.62.+v, 37.10.Ty, 42.50.Cz

## Some Calculable Contributions to Holographic Entanglement Entropy

Ling-Yan Hung, Robert C. Myers and Michael Smolkin

*Perimeter Institute for Theoretical Physics,*

*31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*

**ABSTRACT:** Using the AdS/CFT correspondence, we examine entanglement entropy for a boundary theory deformed by a relevant operator and establish two results. The first is that if there is a contribution which is logarithmic in the UV cut-off, then the coefficient of this term is independent of the state of the boundary theory. In fact, the same is true of all of the coefficients of contributions which diverge as some power of the UV cut-off. Secondly, we show that the relevant deformation introduces new logarithmic contributions to the entanglement entropy. The form of some of these new contributions is similar to that found recently in an investigation of entanglement entropy in a free massive scalar field theory [1].

## Background independent condensed matter models for quantum gravity

Allodia Hamma<sup>1</sup> and Fotis Markopoulou<sup>1,2,4</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, 31 Caroline St. N. N2L 2Y5 Waterloo ON, Canada*

<sup>2</sup>*Department of Physics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

<sup>3</sup>*Max-Planck-Institut für Gravitationsphysik (Albert-Einstein-Institut), Am Mühlenberg 1, D-14476 Golm, Germany*

<sup>4</sup>*Santa Fe Institute, 1515 Hyde Park Road, SF 808 Santa Fe, USA*

A number of recent proposals for a quantum theory of gravity are based on the idea that spacetime geometry and gravity are derivative concepts and only apply at an approximate level. There are two fundamental challenges to any such approach. At the conceptual level, there is a clash between the ‘finiteness’ of general relativity and emergence. Second, the lack of a fundamental quantum makes difficult the straightforward application of well-known methods of statistical physics to the problem. We recently initiated a study of such problems using spin systems based on evaluation of quantum networks with no a priori geometric notions as models for emergent geometry and gravity.

In this article we review two such models. The first is a model of emergent (flat) space and matter and we show how to use methods from quantum information theory to derive features such as speed of light from a non-geometric quantum system. The second model exhibits interacting matter and geometry, with the geometry defined by the behavior of matter. This model has primitive notions of gravitational attraction which we illustrate with a toy black hole, and exhibits entanglement between matter and geometry and thermalization of the quantum geometry.

PACS numbers:

Niv:1105.6055v1 [hep-th] 30 May 2011

26 Nov 2010

25v2 [hep-th] 21 Sep 2007

-ph] 2 Aug 2010







# Quantum Information in Foundational Physics

## Black holes as mirrors: quantum information in random subsystems

Patrick Hayden

*School of Computer Science, McGill University, Montreal, Quebec, H3A 2A7, Canada*

John Preskill

*Institute for Quantum Information, California Institute of Technology, Pasadena CA 91125, USA*

### Abstract

We study information retrieval from evaporating black holes, assuming that the internal dynamics of a black hole is unitary and rapidly mixing, and assuming that the retriever has unlimited control over the emitted Hawking radiation. If the evaporation of the black hole has already proceeded past the ‘half-way’ point, where half of the initial entropy has been radiated away, then additional quantum information deposited in the black hole is revealed in the Hawking radiation very rapidly. Information deposited prior to the half-way point remains concealed until the half-way point, and then emerges quickly. These conclusions hold because typical local quantum circuits are efficient encoders for quantum error-correcting codes that nearly achieve the capacity of the quantum erasure channel. Our estimate of a black hole’s information retention time, based on speculative dynamical assumptions, is just barely compatible with the black hole complementarity hypothesis.

## Simulating quantum effects of cosmological expansion using a static ion trap

Nicolas C. Menicucci,<sup>1</sup> S. Jay Olson,<sup>2</sup> and Gerard J. Milburn<sup>2</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada*

<sup>2</sup>*Centre for Quantum Computer Technology, School of Mathematics and Physics,  
The University of Queensland, St Lucia, QLD, 4072, Australia*

(Date: August 2, 2010)

We propose a new experimental setup that uses ions in the collective ground state of a static trap for studying the analog of quantum-field effects in cosmological spacetimes, including the Gibbons-Hawking effect for a single detector in de Sitter spacetime, as well as the possibility of modeling inflationary structure formation and the entanglement signature of de Sitter spacetime. To date, proposals for using trapped ions in analog gravity experiments have simulated the effect of gravity on the field modes by directly manipulating the ions’ motion. In contrast, by associating laboratory time with conformal time in the simulated universe, we can encode the full effect of curvature in the modulation of the laser used to couple the ions’ vibrational motion and electronic states. This model simplifies the experimental requirements for modeling the analog of an expanding universe using trapped ions and enlarges the validity of the ion-trap analogy to a wide range of interesting cases.

PACS numbers: 03.65.-w, 04.62.+v, 37.10.Ty, 42.50.Cz

## Some Calculable Contributions to Holographic Entanglement Entropy

Ling-Yan Hung, Robert C. Myers and Michael Smolkin

*Perimeter Institute for Theoretical Physics,*

*31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*

**ABSTRACT:** Using the AdS/CFT correspondence, we examine entanglement entropy for a boundary theory deformed by a relevant operator and establish two results. The first is that if there is a contribution which is logarithmic in the UV cut-off, then the coefficient of this term is independent of the state of the boundary theory. In fact, the same is true of all of the coefficients of contributions which diverge as some power of the UV cut-off. Secondly, we show that the relevant deformation introduces new logarithmic contributions to the entanglement entropy. The form of some of these new contributions is similar to that found recently in an investigation of entanglement entropy in a free massive scalar field theory [1].

## Background independent condensed matter models for quantum gravity

Allencia Hamma<sup>1</sup> and Fotis Markopoulou<sup>1,2,4</sup>

<sup>1</sup>*Perimeter Institute for Theoretical Physics, 31 Caroline St. N. N2L 2Y5 Waterloo ON, Canada*

<sup>2</sup>*Department of Physics, University of Waterloo, Waterloo, Ontario N2L 2G1, Canada*

<sup>3</sup>*Max-Planck-Institute für Gravitationsphysik (Albert Einstein Institute), Am Mühlenberg 1, D-14476 Golm, Germany*

<sup>4</sup>*Simon Stevin Institute, 1000 Hyde Park Road, 47500 Suttons Pt, USA*

A number of recent proposals for a quantum theory of gravity are based on the idea that spacetime geometry and gravity are derivative concepts and only apply at an approximate level. There are two fundamental challenges to any such approach. At the conceptual level, there is a clash between the ‘‘emergence’’ of general relativity and emergence. Second, the lack of a fundamental quantum makes difficult the straightforward application of well-known methods of statistical physics to the problem. We recently initiated a study of such problems using spin systems based on evaluation of quantum networks with no a priori geometric notions as models for emergent geometry and gravity.

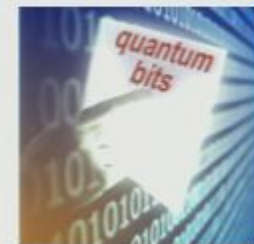
In this article we review two such models. The first is a model of emergent (flat) space and matter and we show how to use methods from quantum information theory to derive features such as speed of light from a non-geometric quantum system. The second model exhibits interacting matter and geometry, with the geometry defined by the behavior of matter. This model has primitive notions of gravitational attraction which we illustrate with a toy black hole, and exhibits entanglement between matter and geometry and thermalization of the quantum geometry.

PACS numbers:

# Conclusions

# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.



[cordis.europa.eu](http://cordis.europa.eu)

# Conclusions

# Quantum Information in Foundational Physics

(see del Rio and Deivat talks)

## Black holes as mirrors: quantum information in random subsystems

Patrick Hayden

School of Computer Science, McGill University, Montreal, Quebec, H3A 2A7, Canada

John Preskill

Institute for Quantum Information, California Institute of Technology, Pasadena CA 91125, USA

### Abstract

We study information retrieval from evaporating black holes, assuming that the internal dynamics of a black hole is unitary and rapidly mixing, and assuming that the retriever has unlimited control over the emitted Hawking radiation. If the evaporation of the black hole has already proceeded past the ‘half-way’ point, where half of the initial entropy has been radiated away, then additional quantum information deposited in the black hole is revealed in the Hawking radiation very rapidly. Information deposited prior to the half-way point remains concealed until the half-way point, and then emerges quickly. These conclusions hold because typical local quantum circuits are efficient encoders for quantum error-correcting codes that nearly achieve the capacity of the quantum erasure channel. Our estimate of a black hole’s information retention time, based on speculative dynamical assumptions, is just barely compatible with the black hole complementarity hypothesis.

## Simulating quantum effects of cosmological expansion using a static ion trap

Nicolas C. Menicucci,<sup>1</sup> S. Jay Olson,<sup>2</sup> and Gerard J. Milburn<sup>2</sup>

<sup>1</sup>Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada

<sup>2</sup>Centre for Quantum Computer Technology, School of Mathematics and Physics,  
The University of Queensland, St. Lucia, QLD, 4072, Australia

(Date: August 2, 2010)

We propose a new experimental setup that uses ions in the collective ground state of a static trap for studying the analog of quantum-field effects in cosmological spacetimes, including the Gibbons-Hawking effect for a single detector in de Sitter spacetime, as well as the possibility of modeling inflationary structure formation and the entanglement signature of de Sitter spacetime. To date, proposals for using trapped ions in analog gravity experiments have simulated the effect of gravity on the field modes by directly manipulating the ions’ motion. In contrast, by associating laboratory time with conformal time in the simulated universe, we can encode the full effect of curvature in the modulation of the laser used to couple the ions’ vibrational motion and electronic states. This model simplifies the experimental requirements for modeling the analog of an expanding universe using trapped ions and enlarges the validity of the ion-trap analogy to a wide range of interesting cases.

PACS numbers: 03.65.-w, 04.02.+x, 37.10.Ty, 42.50.Cx

## Some Calculable Contributions to Holographic Entanglement Entropy

Ling-Yan Hung, Robert C. Myers and Michael Smolkin

Perimeter Institute for Theoretical Physics,

31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada

**ABSTRACT:** Using the AdS/CFT correspondence, we examine entanglement entropy for a boundary theory deformed by a relevant operator and establish two results. The first is that if there is a contribution which is logarithmic in the UV cut-off, then the coefficient of this term is independent of the state of the boundary theory. In fact, the same is true of all of the coefficients of contributions which diverge as some power of the UV cut-off. Secondly, we show that the relevant deformation introduces new logarithmic contributions to the entanglement entropy. The form of some of these new contributions is similar to that found recently in an investigation of entanglement entropy in a free massive scalar field theory [1].

## Background independent condensed matter models for quantum gravity

Allencia Hamma<sup>1</sup> and Fotis Markopoulou<sup>1,2,4</sup>

<sup>1</sup>Perimeter Institute for Theoretical Physics, 31 Caroline St. N. N2L 2Y5, Waterloo ON, Canada

<sup>2</sup>Department of Physics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

<sup>3</sup>Max-Planck-Institute für Gravitationsphysik (Albert-Einstein-Institut), Am Mühlenberg 1, D-14476 Golm, Germany

<sup>4</sup>Simon Stevin Institute, 1000 Hyde Park Road, 4F503 Santa Fe, USA

A number of recent proposals for a quantum theory of gravity are based on the idea that spacetime geometry and gravity are derivative concepts and only apply at an approximate level. There are two fundamental challenges to any such approach. At the conceptual level, there is a clash between the ‘finiteness’ of general relativity and emergence. Second, the lack of a fundamental quantum makes difficult the straightforward application of well-known methods of statistical physics to the problem. We recently initiated a study of such problems using spin systems based on evaluation of quantum networks with no a priori geometric notions as models for emergent geometry and gravity.

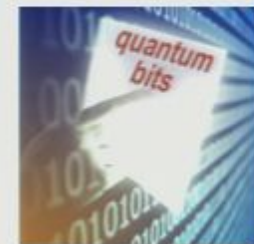
In this article we review two such models. The first is a model of emergent (flat) space and matter and we show how to use methods from quantum information theory to derive features such as speed of light from a non-geometric quantum system. The second model exhibits interacting matter and geometry, with the geometry defined by the behavior of matter. This model has primitive notions of gravitational attraction which we illustrate with a toy black hole, and exhibits entanglement between matter and geometry and thermalization of the quantum geometry.

PACS numbers:

# Conclusions

# Conclusions

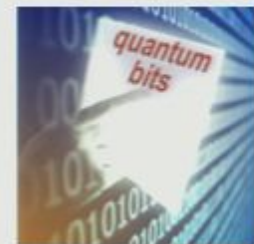
- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.



[cordis.europa.eu](http://cordis.europa.eu)

# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.

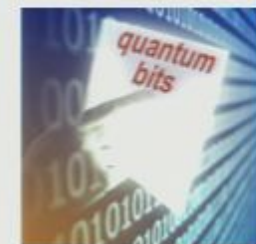


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.
- Large scale quantum information processors seem possible; technologically very challenging to realize. This is a major focus for experimental physics today.

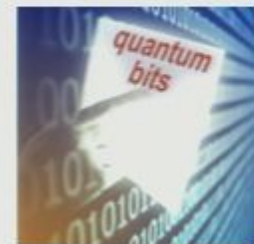


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.

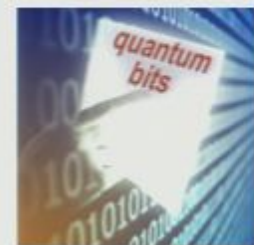


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.
- Large scale quantum information processors seem possible; technologically very challenging to realize. This is a major focus for experimental physics today.

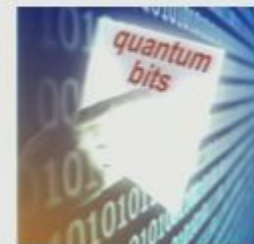


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.

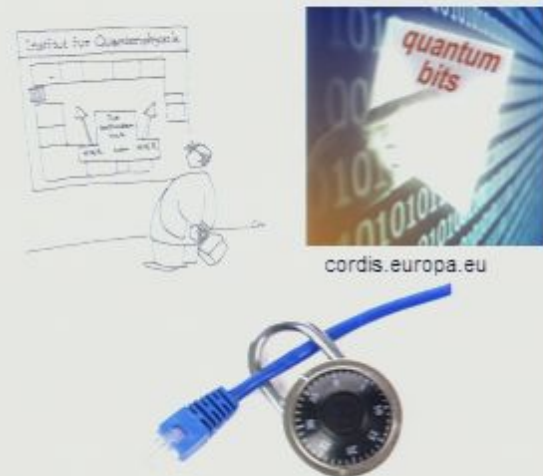


[cordis.europa.eu](http://cordis.europa.eu)



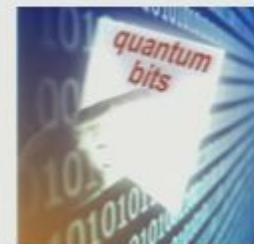
# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.
- Large scale quantum information processors seem possible; technologically very challenging to realize. This is a major focus for experimental physics today.



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.

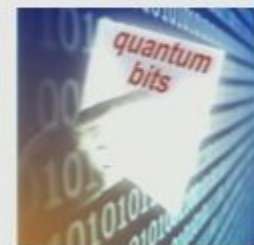


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.
- Large scale quantum information processors seem possible; technologically very challenging to realize. This is a major focus for experimental physics today.

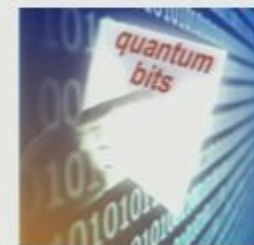


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.
- Large scale quantum information processors seem possible; technologically very challenging to realize. This is a major focus for experimental physics today.
- Quantum mechanics offers a valuable new primitive for cryptography: intrinsic eavesdropper detection. Quantum key distribution is already possible.

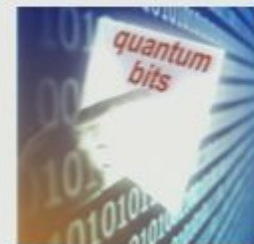


[cordis.europa.eu](http://cordis.europa.eu)



# Conclusions

- The world is quantum mechanical. This changes our understanding of what information is, and what we can do with it.
- Quantum information processing redefines what is computationally hard or easy. This changes the rules of the game for “computationally secure” cryptography.
- Large scale quantum information processors seem possible; technologically very challenging to realize. This is a major focus for experimental physics today.
- Quantum mechanics offers a valuable new primitive for cryptography: intrinsic eavesdropper detection. Quantum key distribution is already possible.



cordis.europa.eu



# Supporters ...



Canada Foundation  
for Innovation

Fondation canadienne  
pour l'innovation



Ontario Centres of  
Excellence



Canada



Ontario



**NSERC  
CRSNG**



**CIFAR**

CANADIAN INSTITUTE  
for ADVANCED RESEARCH



# Research Opportunities at IQC

## **Student Positions**

- Research toward Master and PhD degrees
- Undergraduate Projects & Internships
- EU Exchange Program
- Summer Programs
  - Undergraduate School on Experimental Quantum Information Processing
  - Quantum Cryptography School for Young Students

## **Faculty Positions**

- Faculty of Engineering
- Faculty of Mathematics
- Faculty of Science
- Research (Assistant or Associate) Professorship

## **Postdoctoral Fellowships**

- IQC Postdoctoral Fellowship
- Postdoctoral Fellowship on Quantum Circuits

Visit [iqc.uwaterloo.ca/welcome/positions](http://iqc.uwaterloo.ca/welcome/positions) for more

# Research Opportunities at IQC

## **Student Positions**

- Research toward Master and PhD degrees
- Undergraduate Projects & Internships
- EU Exchange Program
- Summer Programs
  - Undergraduate School on Experimental Quantum Information Processing
  - Quantum Cryptography School for Young Students

## **Faculty Positions**

- Faculty of Engineering
- Faculty of Mathematics
- Faculty of Science
- Research (Assistant or Associate) Professorship

## **Postdoctoral Fellowships**

- IQC Postdoctoral Fellowship
- Postdoctoral Fellowship on Quantum Circuits

Visit [iqc.uwaterloo.ca/welcome/positions](http://iqc.uwaterloo.ca/welcome/positions) for more