University of Glasgow | Department of Computing Science

Formal Analysis of Quantum Systems using Process Calculus

Simon Gay
University of Glasgow

Quantum Computing in the Media

Quantum computer to debut next week - Techworld.com

http://news.techworld.com/operating-systems/7972/quantum-computer-to-debut-next-week/

Home > News

Operating Systems Feed

Quantum computer to debut next week

Could this crack all our codes?

By Peter Judge | Techworld
Published: 00:10 GMT, 08 February 07

Twenty years before most scientists expected it, a commercial company has announced a quantum computer that promises to massively speed up searches and optimisation calculations.

D-Wave of British Columbia has promised to demonstrate a quantum computer next Tuesday, that can carry out 64,000 calculations simultaneously (in parallel "universes"), thanks to a new technique which rethinks the already-uncanny world of quantum computing. But the academic world is taking a wait-and-see approach.

D-Wave is the world's only "commercial" quantum computing company, backed by more than $20 million of venture capital (there are more commercial ventures in the related field of quantum cryptography). Its stated aim is to eventually produce commercially available quantum computers that can be used online or shipped to computer rooms, where they will solve intractable and expensive problems such as financial optimisation.

Related Content

Features

Simplify your enterprise Windows 7 migration

Why cult madness is driving me off Apple

The worst things about Windows 7

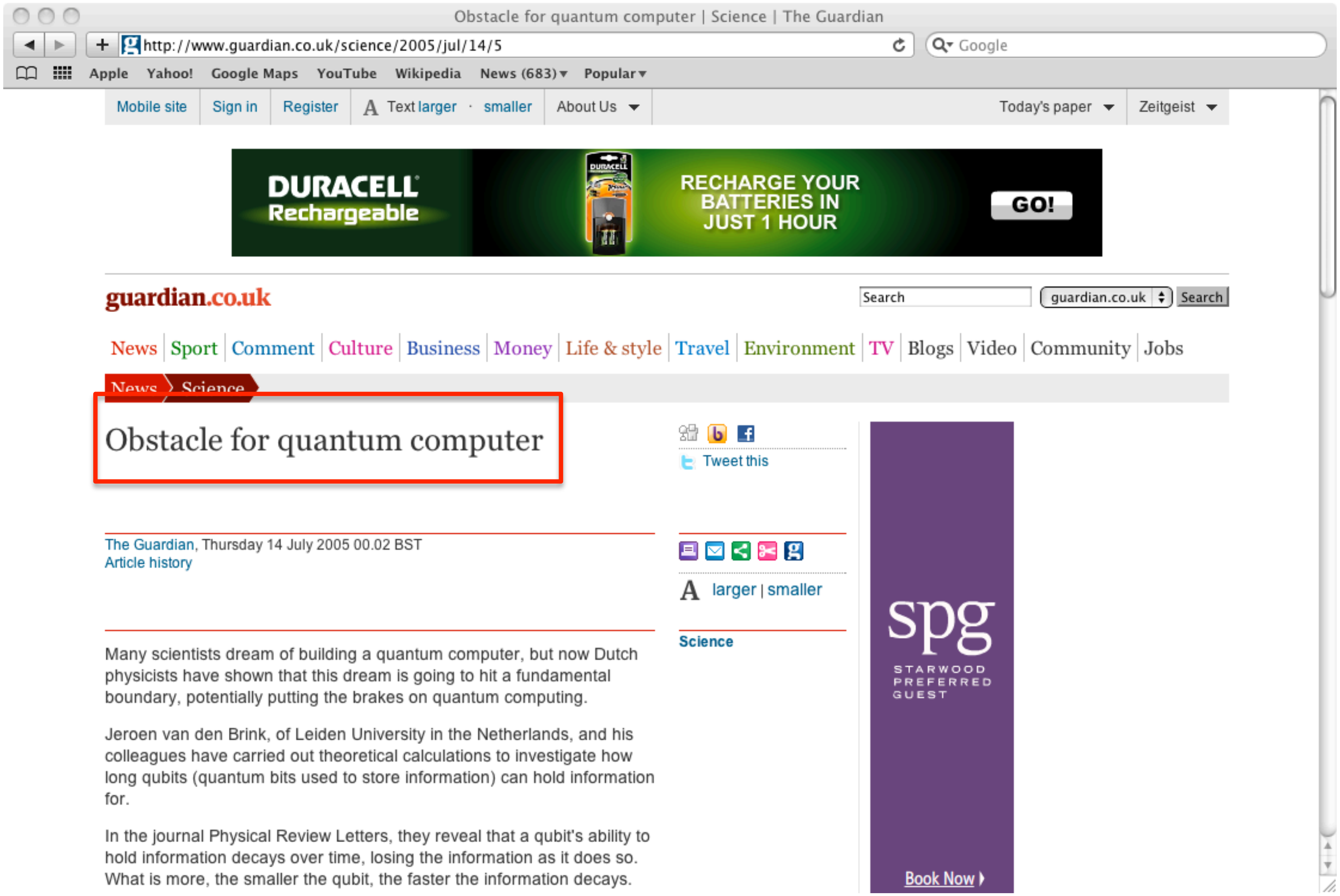
Top business articles

16 breakthrough notebooks: A look back

Microsoft to kill business server package

Google Apps backup is ideal for small business

Quantum Computing in the Media



Obstacle for quantum computer | Science | The Guardian

http://www.guardian.co.uk/science/2005/jul/14/5

guardian.co.uk

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | TV | Blogs | Video | Community | Jobs

News > Science

Obstacle for quantum computer

The Guardian, Thursday 14 July 2005 00.02 BST
Article history

Many scientists dream of building a quantum computer, but now Dutch physicists have shown that this dream is going to hit a fundamental boundary, potentially putting the brakes on quantum computing.

Jeroen van den Brink, of Leiden University in the Netherlands, and his colleagues have carried out theoretical calculations to investigate how long qubits (quantum bits used to store information) can hold information for.

In the journal Physical Review Letters, they reveal that a qubit's ability to hold information decays over time, losing the information as it does so. What is more, the smaller the qubit, the faster the information decays.

Quantum Computing in the Media

Hey presto! the quantum supercomputer – Science, News – The Independent

http://www.independent.co.uk/news/science/hey-presto-the-quantum-supercomputer-738720.ht

Apple Yahoo! Google Maps YouTube Wikipedia News (683) Popular

QUEEN RANIA OF JORDAN: HARDLINERS ARE NOW THE FACE OF ISRAEL

THE INDEPENDENT SCIENCE

17° London Hi 21°C / Lo 11°C

Search The Independent with Google Go Popular Topics

FOOTBALL EMAIL The latest action straight to your inbox

CenterParcs to relaxing ...

News | Opinion | Environment | Sport | Life & Style | Arts & Entertainment | Travel | Money | IndyBest | Student | Shopping

UK World Business People Science Media Education Obituaries Video Corrections Weather News Wall myIndependent

Home > News > Science

Hey presto! the quantum supercomputer

Mythical cats in boxes? Time travel? How about computers as powerful as the Universe? We're talking quantum physics. And now the technology is with us

By John Gribbin

Friday, 19 November 1999

SHARE | PRINT | EMAIL | AAA TEXT SIZE

Quantum physics used to be exotic science. It is now technology. That doesn't mean that we understand it - as Richard Feynman, one of the greatest quantum mechanics, was fond of saying, "nobody understands quantum physics". Don't try to understand how the quantum world can be the way it is, he urged; just lie back and enjoy it.

Quantum physics used to be exotic science. It is now technology. That doesn't mean that we understand it - as Richard Feynman, one of the greatest quantum mechanics, was fond of saying, "nobody understands quantum physics". Don't try to understand how the quantum world can be the way it is, he urged; just lie back and enjoy it.

It means that engineers have learnt how to manipulate quantum entities, such as single atoms, using the same kind of empirical, suck-it-and-see approach that enabled engineers to design effective steam engines long before the laws of

EDITOR'S CHOICE

Gorbachev: Russia's elder statesman

Gladiatorial relics discovered in York

Banksy makes his mark across America

Danny Boyle to direct 2012 ceremony

Quantum Computing in the Media

Quantum Computing in the Media

Will the QC kill the PC? – Telegraph

http://www.telegraph.co.uk/science/science-news/3345943/Will-the-QC-kill-the-PC.html

Monday 07 June 2010 | Science News feed

Log in | Register now

Pay Monthly The next hot shot Virgin media

Telegraph.co.uk

Home | News | Sport | Finance | Lifestyle | Comment | Travel | Culture | Technology | Fashion | Jobs | Dating | Subscriber | Offers

UK | World | Politics | Celebrities | Obituaries | Weird | Earth | Science | Health News | Education | Topics | News Blogs | News Video

Science News | Space | Dinosaurs | Evolution | Steve Jones | Science Picture Galleries

Will the QC kill the PC?

Richard Gray
Published: 12:01AM BST 01 Jul 2008

Will the PC soon become a thing of the past?

Quantum computers could become a reality very soon, opening up some fantastic possibilities - including teleportation, says Richard Gray

Why we should celebrate Charles Darwin
Solving the riddle of the Tunguska Event
Telegraph science | Telegraph Digital Life

It might be the science of the very small, but quantum computing is on the verge of solving some giant problems. For more than 30 years, physicists have dreamed of harnessing the power of atoms to produce computers that would far outstrip the capabilities of the silicon microchips used in today's PCs.

These machines would have the ability to perform calculations that would take normal computers millions of years, while carrying out a vast number of tasks simultaneously. They promise to make as big

Related Articles
Northern Ireland parade for Queen's Royal Hussars

Share | Digg submit | 0 tweet | Email | Print | Text Size

Science News
Earth
New species found

SCIENTIFIC JOBS
Study Director - Bioanalytical Services
Harrogate, On Application
Programme Manager
North West, £35000 - £40000
Key Account Manager
East Anglia, £30000 - £40000
Upload your CV | Career advice
Get job alerts | Advertise a job

The Open University

Quantum Computing in the Media

BBC NEWS | Science & Environment | Quantum computer slips onto chips

http://news.bbc.co.uk/1/hi/sci/tech/8236943.stm

Apple Yahoo! Google Maps YouTube Wikipedia News (683) Popular

Mobile Version | Help

BBC Home News Sport Weather iPlayer TV Radio More... Search

NEWS LIVE BBC NEWS CHANNEL

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports

Related BBC sites
Sport
Weather

Page last updated at 11:12 GMT, Friday, 4 September 2009 12:12 UK

E-mail this to a friend   Printable version

Quantum computer slips onto chips

Researchers have devised a penny-sized silicon chip that uses photons to run Shor's algorithm - a well-known quantum approach - to solve a maths problem.

The algorithm computes the two numbers that multiply together to form a given figure, and has until now required laboratory-sized optical computers.

Chips like this one could form the basis for future optical computers

This kind of factoring is the basis for a wide variety of encryption schemes.

The work, reported in Science, is rudimentary but could easily be scaled up to handle more complex computing.

Shor's algorithm and the factoring of large numbers has been a particular case used to illustrate the power of quantum computing.

Quantum computers exploit the counterintuitive fact that photons or trapped atoms can exist in multiple states or "superpositions" at the same time.

SEE ALSO
- Bridging the gap to quantum world
  03 Jun 09 | Science & Environment
- Major leap for faster computers
  19 Mar 09 | Edinburgh, East and Fife
- 'Unbreakable' encryption unveiled
  09 Oct 08 | Science & Environment
- Quantum computing
  13 Nov 07 | Technology
- Optical computing
  13 Nov 07 | Technology

RELATED INTERNET LINKS
- Science
- Bristol University

The BBC is not responsible for the content of external internet sites

TOP SCIENCE & ENVIRONMENT STORIES
- Brain scan 'lie detector' warning
- Humpback whales form friendships
- Climate wiped out Europe's apes

University of Glasgow

Aims of This Talk

I will try to answer the following questions.

- **What is quantum information processing?**
- **Why is it interesting?**
- **Why do I want to apply formal methods?**
- **What can be done with quantum process calculus?**

Acknowledgements: Collaborators

Dr Raja Nagarajan, University of Warwick

Dr Nick Papanikolaou, Hewlett-Packard Labs

Tim Davidson, University of Warwick

Dr Hynek Mlnařík, University of Warwick

Dr Ian Mackie, University of Sussex

Dr Paulo Mateus, Technical University of Lisbon

Dr Pedro Adão, Technical University of Lisbon

Dr Sonja Franke-Arnold, University of Glasgow

Ittoop Vergheese Puthoor, University of Glasgow

Acknowledgements: Funding

QNET: Network on Semantics of Quantum Computation (EPSRC 2006-2010)

QFOX: Quantum Computation: Foundations, Security, Cryptography and Group Theory (EPSRC 2008-2011)

Lord Kelvin / Adam Smith PhD Scholarship (University of Glasgow)

QUISCO (Quantum Information Science Scotland)

What is Quantum Information Processing?

The idea is to represent information by means of physical systems whose behaviour must be described by quantum physics, and to process information by means of operations that arise from quantum physics.

Examples: the spin state of a single atom
the polarization state of a single photon

Superposition

The state of a classical bit is either 0 or 1.
The state of a quantum bit (qubit) is

$$\alpha|0\rangle + \beta|1\rangle$$

where $|0\rangle$ **and** $|1\rangle$ **are the basis states.**

For example: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ **or** $\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$

A qubit may be in a basis state or it may be in a superposition state.

Measurement

It is not possible to inspect the components of a quantum state. We can only do a measurement.

Measuring a qubit that is in state $\alpha|0\rangle + \beta|1\rangle$

has a random result:

with probability $|\alpha|^2$ **the result is** $|0\rangle$

with probability $|\beta|^2$ **the result is** $|1\rangle$

Operations on a Superposition

An operation acts on every basis state in the superposition. For example, if we have the state

$$\frac{1}{2}|000\rangle + \frac{1}{2}|010\rangle - \frac{1}{2}|110\rangle - \frac{1}{2}|111\rangle$$

and we apply the operation "invert the second bit" then we get the state

$$\frac{1}{2}|010\rangle + \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle - \frac{1}{2}|101\rangle$$

Note that a measurement does not allow us to discover the result of applying the operation to every basis state.

No Cloning

It is not possible to define an operation that reliably makes a duplicate of an unknown quantum state.

(Contrast this with the classical situation, where the existence of uniform copying procedures is one of the main advantages of digital information.)

It is possible to transfer an unknown quantum state from one physical carrier to another, but the process destroys the original. This is known as quantum teleportation.

Entanglement

The states of two (or more) qubits can be correlated in a way that is stronger than any possible classical correlation. This is known as quantum entanglement.

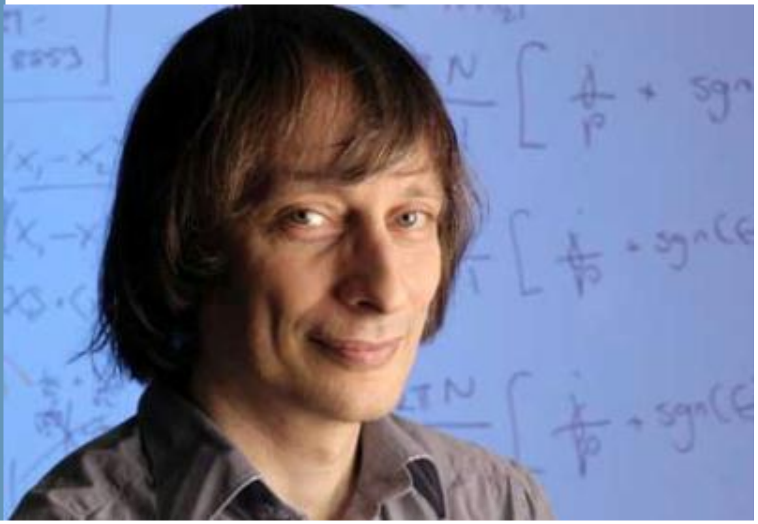
Many quantum algorithms and communication protocols make use of entanglement.

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Deutsch-Jozsa Algorithm (David Deutsch / Richard Jozsa, 1992)

Given a function $f:\{0,1\}^n \rightarrow \{0,1\}$ that is either constant or balanced, works out which, with only one evaluation of f .

A classical algorithm would require $2^{n-1}+1$ evaluations in the worst case.



Shor's Algorithm (Peter Shor, 1994)

A quantum algorithm for factorising integers, which is more efficient than any known classical algorithm.

$$(\log n)^3 \quad vs. \quad e^{(\log n)^{1/3}(\log \log n)^{2/3}}$$

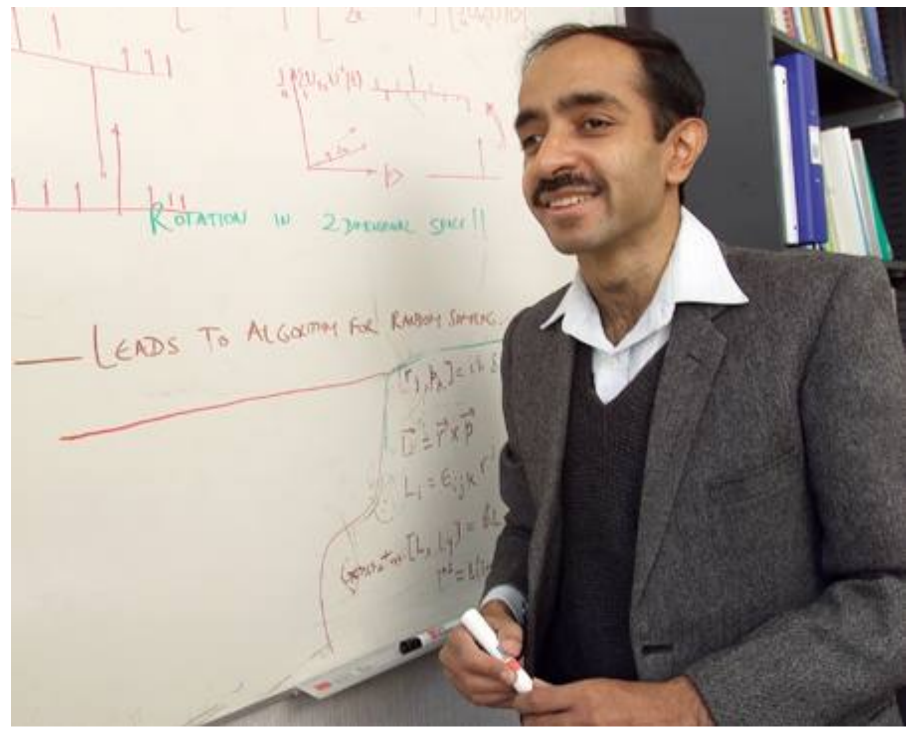
The RSA cryptosystem used for internet security relies on the assumption that factorisation is difficult. A practical implementation of Shor's algorithm would threaten current information security technology.

However, factorisation is believed not to be a member of the class of intractable problems known as NP-complete problems.

Grover's Algorithm (Lov Grover, 1996)

A quantum search algorithm. It requires $\sqrt{n}$ steps to find an item in an unstructured list of length n.

Classically, every item must be inspected, requiring $n/2$ operations on average.



BB84 (Charles Bennett & Gilles Brassard, 1984)

A protocol for generating shared cryptographic keys. Its security relies only on the laws of quantum physics, especially the no-cloning principle. It is secure against all possible future developments in quantum computing.

University of Glasgow

Why is Quantum Computing Interesting?

It is interesting to understand the information-processing power permitted by the laws of physics.

Quantum algorithms might help to solve some classes of problem more efficiently.

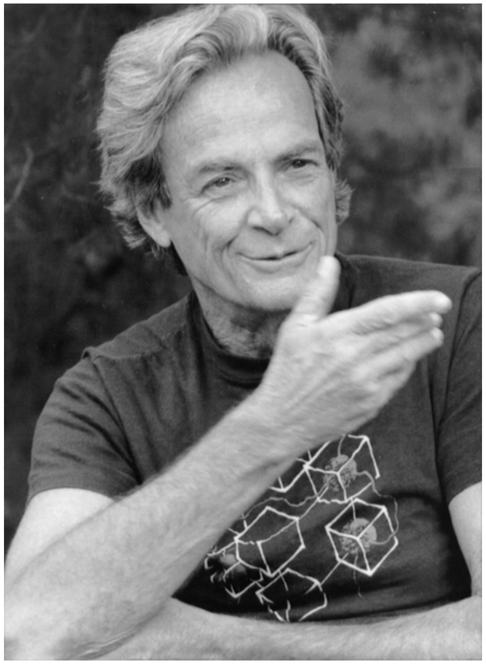
> **But if NP-complete problems cannot be solved efficiently even by a quantum computer, understanding why not is also of fundamental interest.**

Quantum cryptography deals with any threat that quantum computing poses to classical cryptography.

Why is Quantum Computing Interesting?

As integrated circuit components become smaller, quantum effects become difficult to avoid. Quantum computing might be necessary in order to continue making computers smaller.

Richard Feynman (1982) suggested that quantum computers could be used to simulate complex (quantum) physical systems, whose behaviour is difficult to analyse.



Will QIP Become Practically Significant?

Will QIP Become Practically Significant?

Will QIP Become Practically Significant?


http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf

MAGIQ QPN™ 8505
Security Gateway
Uncompromising VPN Security™

Carrier Class Network Security

- Quantum Key Distribution
- Key refresh rate up to 100 256 bit keys a second
- Intrusion Detection
- Always-on base VPN
- Data protection with best of breed encryption technologies
- In-transit data security
- Network compatibility
- Implements industry standards BB84, 3DES, AES
- Integrated encryption and Quantum Key Distribution in one enclosure

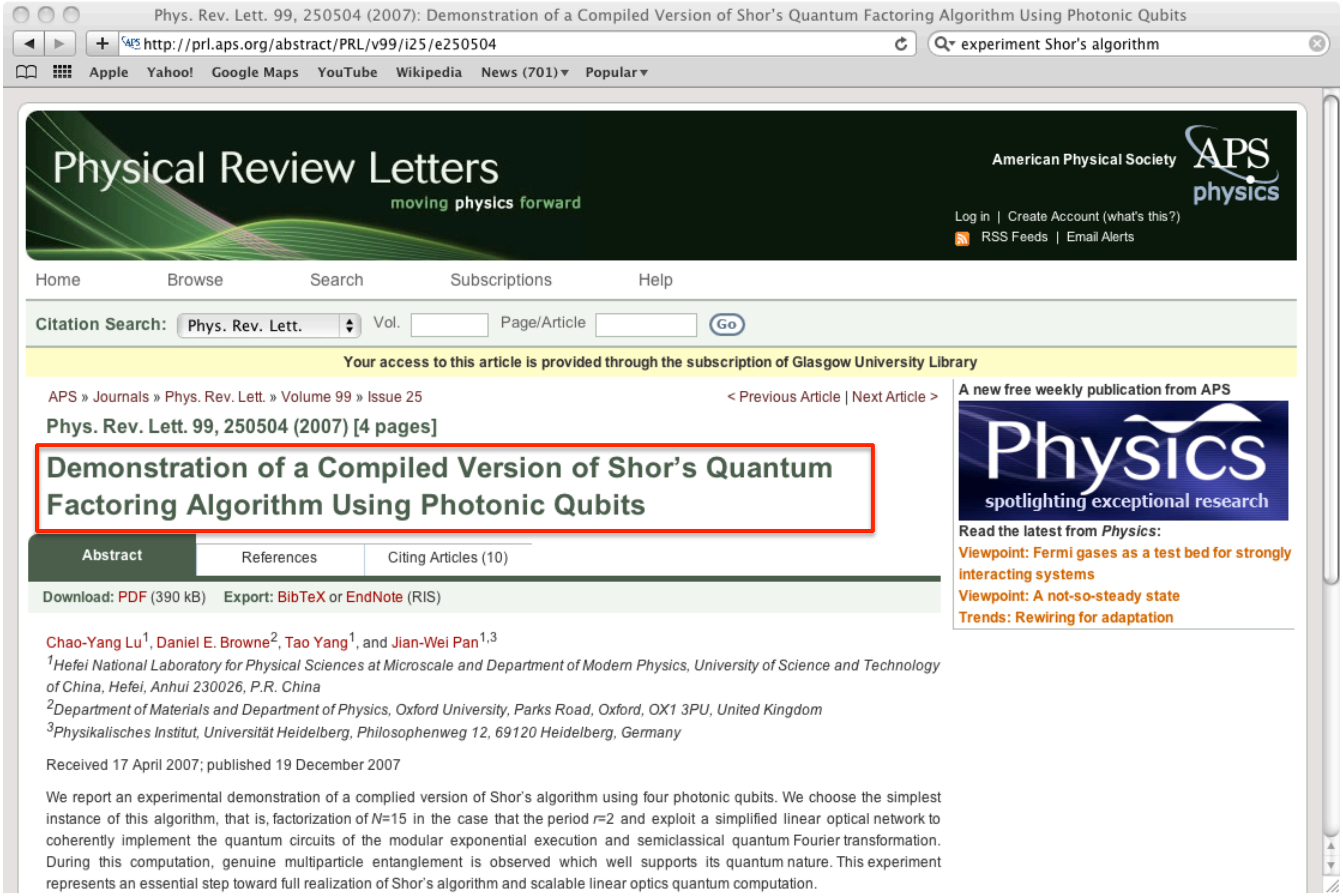
OVERVIEW

Technology companies have responded to heightened requirements for information security with an avalanche of new cryptography products. As sophisticated as these solutions are, they have this in common: they all rely on computational difficulty as the source of their protection and none can escape the fact that information security that relies on computational difficulty is ultimately vulnerable.

Breaking through to information security that's NOT VULNERABLE means breaking new ground. Breaking with the tradition of refining current solutions; finding new directions; pioneering completely new technologies that can't be threatened by the next new chip or the next new software algorithm: that's been the mission of MagiQ Technologies since 1999.

Will QIP Become Practically Significant?

Will QIP Become Practically Significant?



Phys. Rev. Lett. 99, 250504 (2007): Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits

http://prl.aps.org/abstract/PRL/v99/i25/e250504

experiment Shor's algorithm

Apple Yahoo! Google Maps YouTube Wikipedia News (701) Popular

Physical Review Letters
moving physics forward

American Physical Society APS physics

Log in | Create Account (what's this?)
RSS Feeds | Email Alerts

Home Browse Search Subscriptions Help

Citation Search: Phys. Rev. Lett. Vol. Page/Article Go

Your access to this article is provided through the subscription of Glasgow University Library

APS » Journals » Phys. Rev. Lett. » Volume 99 » Issue 25

< Previous Article | Next Article >

Phys. Rev. Lett. 99, 250504 (2007) [4 pages]

Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits

Abstract References Citing Articles (10)

Download: PDF (390 kB) Export: BibTeX or EndNote (RIS)

Chao-Yang Lu[1], Daniel E. Browne[2], Tao Yang[1], and Jian-Wei Pan[1,3]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P.R. China*

[2]*Department of Materials and Department of Physics, Oxford University, Parks Road, Oxford, OX1 3PU, United Kingdom*

[3]*Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany*

Received 17 April 2007; published 19 December 2007

We report an experimental demonstration of a complied version of Shor's algorithm using four photonic qubits. We choose the simplest instance of this algorithm, that is, factorization of N=15 in the case that the period r=2 and exploit a simplified linear optical network to coherently implement the quantum circuits of the modular exponential execution and semiclassical quantum Fourier transformation. During this computation, genuine multiparticle entanglement is observed which well supports its quantum nature. This experiment represents an essential step toward full realization of Shor's algorithm and scalable linear optics quantum computation.

A new free weekly publication from APS

Physics
spotlighting exceptional research

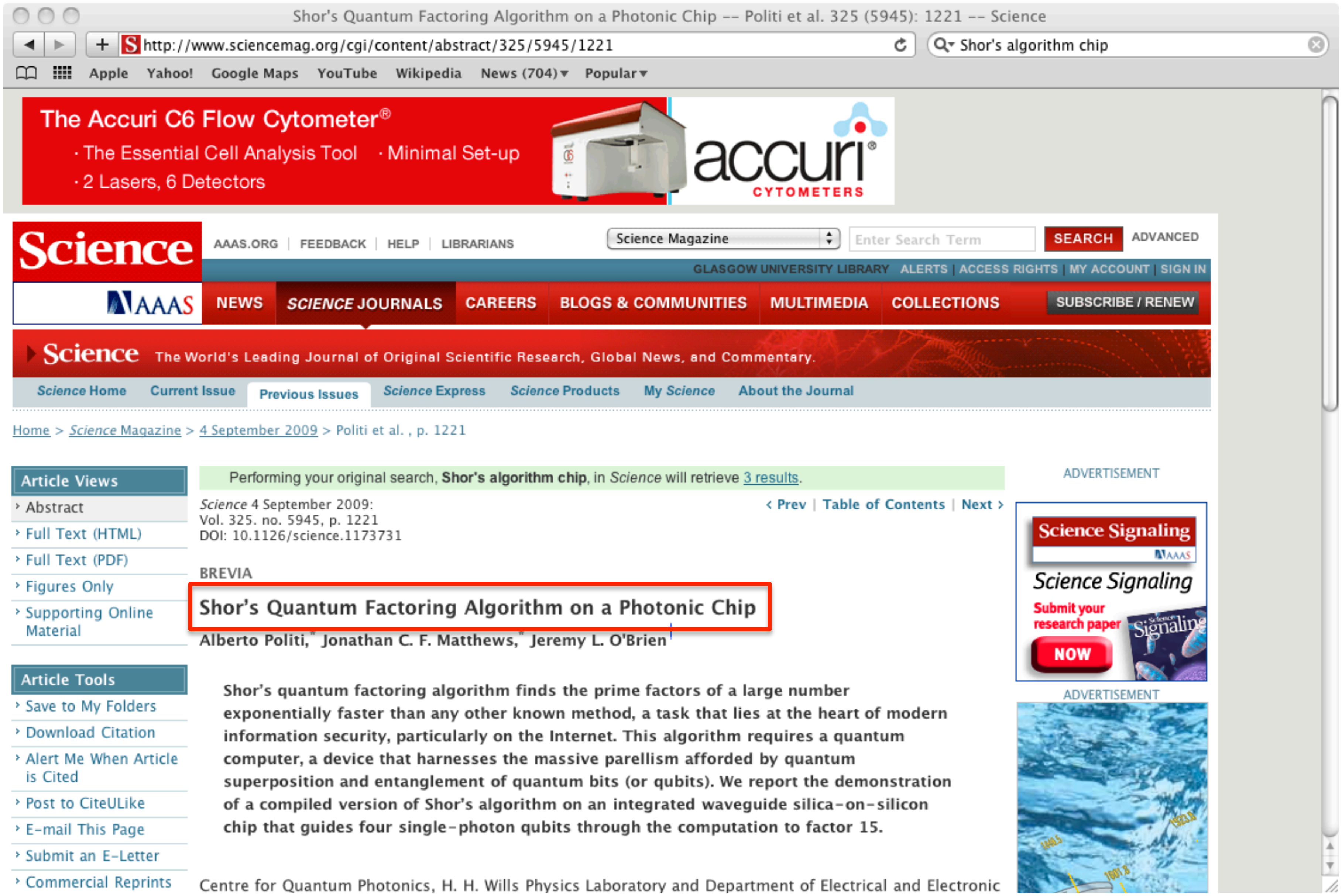
Read the latest from *Physics*:

Viewpoint: Fermi gases as a test bed for strongly interacting systems

Viewpoint: A not-so-steady state

Trends: Rewiring for adaptation

Will QIP Become Practically Significant?



Shor's Quantum Factoring Algorithm on a Photonic Chip -- Politi et al. 325 (5945): 1221 -- Science

http://www.sciencemag.org/cgi/content/abstract/325/5945/1221

Shor's algorithm chip

Apple Yahoo! Google Maps YouTube Wikipedia News (704) Popular

Science AAAS

AAAS.ORG | FEEDBACK | HELP | LIBRARIANS

Science Magazine | Enter Search Term | SEARCH | ADVANCED

GLASGOW UNIVERSITY LIBRARY ALERTS | ACCESS RIGHTS | MY ACCOUNT | SIGN IN

NEWS | *SCIENCE* JOURNALS | CAREERS | BLOGS & COMMUNITIES | MULTIMEDIA | COLLECTIONS | SUBSCRIBE / RENEW

Science The World's Leading Journal of Original Scientific Research, Global News, and Commentary.

Science Home | Current Issue | Previous Issues | *Science* Express | *Science* Products | My *Science* | About the Journal

Home > *Science* Magazine > 4 September 2009 > Politi et al. , p. 1221

Article Views
- Abstract
- Full Text (HTML)
- Full Text (PDF)
- Figures Only
- Supporting Online Material

Article Tools
- Save to My Folders
- Download Citation
- Alert Me When Article is Cited
- Post to CiteULike
- E-mail This Page
- Submit an E-Letter
- Commercial Reprints

Performing your original search, **Shor's algorithm chip**, in *Science* will retrieve 3 results.

Science 4 September 2009:
Vol. 325. no. 5945, p. 1221
DOI: 10.1126/science.1173731

‹ Prev | Table of Contents | Next ›

BREVIA

Shor's Quantum Factoring Algorithm on a Photonic Chip

Alberto Politi,* Jonathan C. F. Matthews,* Jeremy L. O'Brien†

Shor's quantum factoring algorithm finds the prime factors of a large number exponentially faster than any other known method, a task that lies at the heart of modern information security, particularly on the Internet. This algorithm requires a quantum computer, a device that harnesses the massive parellism afforded by quantum superposition and entanglement of quantum bits (or qubits). We report the demonstration of a compiled version of Shor's algorithm on an integrated waveguide silica-on-silicon chip that guides four single-photon qubits through the computation to factor 15.

Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic

University of Glasgow

Will QIP Become Practically Significant?

ScienceDirect – Physics Letters A : Experimental NMR realization of a generalized quantum search algorithm

http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6TVM-43K8V11-R&_user=121723&_cove

experiment Grover's algorithm

Apple Yahoo! Google Maps YouTube Wikipedia News (701) Popular

Home Browse Search My Settings Alerts Help

Quick Search All fields Author

search tips Journal/book title Volume Issue Page Clear Go Advanced Search

Find more full-text articles: Your search for "experiment Grover's algorithm " would return **132** results on ScienceDirect. View Results

Font Size:

PDF (1225 K) Export Citation E-mail Article

Article | Figures/Tables (4) | References (22)

Thumbnails | Full-Size Images

Physics Letters A
Volume 286, Issues 2-3, 23 July 2001, Pages 121-126

doi:10.1016/S0375-9601(01)00416-9 | How to Cite or Link Using DOI

Experimental NMR realization of a generalized quantum search algorithm

G. L. Long[a, b, c, d], H. Y. Yan[a, b], Y. S. Li[a, b], C. C. Tu[a, b], J. X. Tao[a, b], H. M. Chen[a], M. L. Liu[e], X. Zhang[e], J. Luo[e], L. Xiao[a, b, e] and X. Z. Zeng[e]

[a] Department of Physics, Tsinghua University, Beijing 100084, PR China

[b] Key Laboratory for Quantum Information and Measurements, Ministry of Education, Beijing 100084, PR China

[c] Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, PR China

[d] Center of Atomic, Molecular and Nanosciences, Tsinghua University, Beijing 100084, PR China

[e] Laboratory of Magnetic Resonance and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, PR China

Received 6 March 2001; revised 2 May 2001; accepted 12 June 2001 Communicated by P.R. Holland Available online 25 July 2001

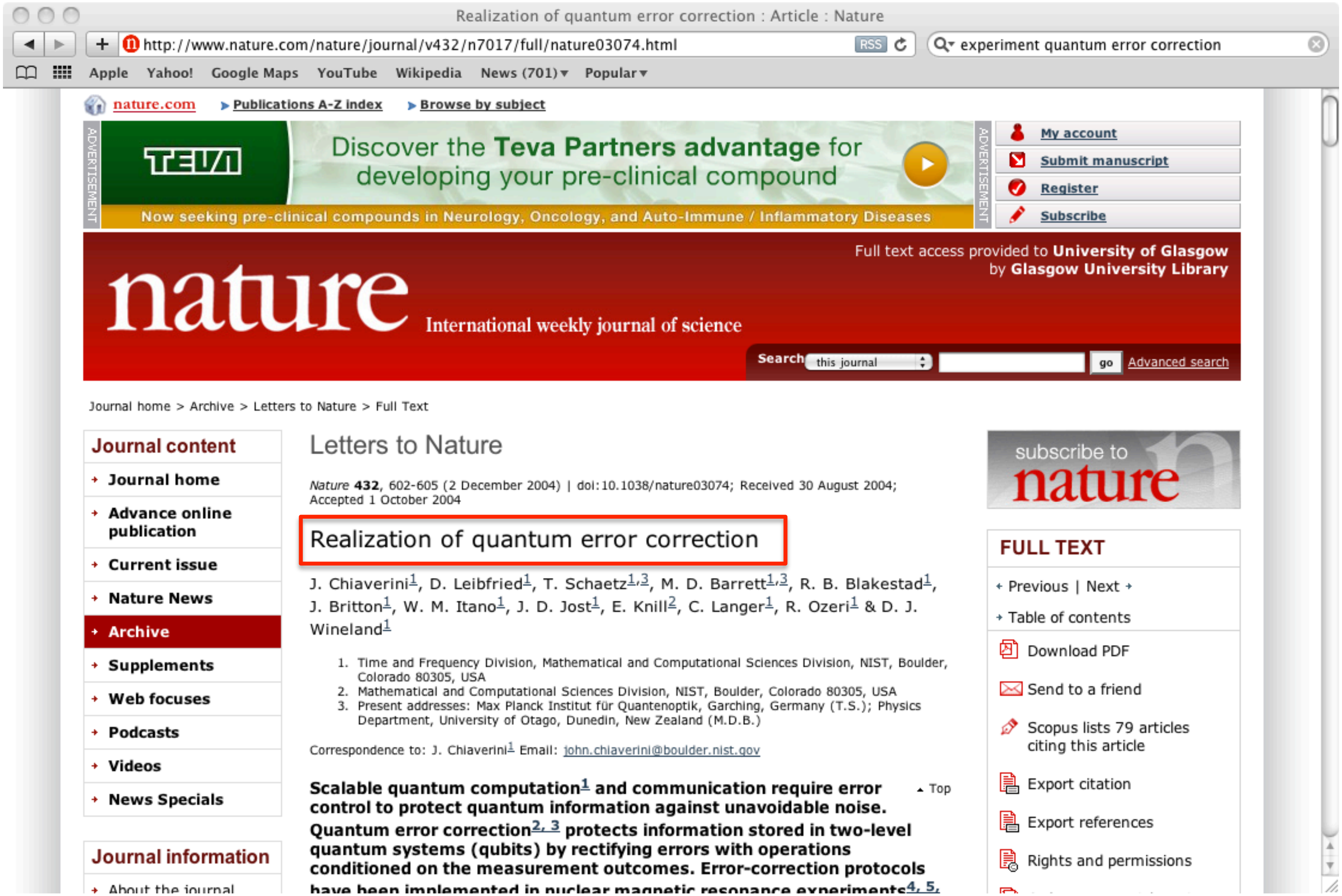
Related Articles

- Phase matching condition for quantum search with a gene... *Physics Letters A*
- Interaction-aided continuous time quantum search *Chaos, Solitons & Fractals*
- Entanglement in the Grover search algorithm *Physics Letters A*

View More Related Articles

View Record in Scopus

Will QIP Become Practically Significant?


Realization of quantum error correction : Article : Nature

http://www.nature.com/nature/journal/v432/n7017/full/nature03074.html

experiment quantum error correction

Apple Yahoo! Google Maps YouTube Wikipedia News (701) Popular

nature.com Publications A-Z index Browse by subject

My account
Submit manuscript
Register
Subscribe

Full text access provided to University of Glasgow by Glasgow University Library

nature
International weekly journal of science

Search this journal go Advanced search

Journal home > Archive > Letters to Nature > Full Text

Journal content
- Journal home
- Advance online publication
- Current issue
- Nature News
- Archive
- Supplements
- Web focuses
- Podcasts
- Videos
- News Specials

Journal information
- About the journal

Letters to Nature

Nature **432**, 602-605 (2 December 2004) | doi:10.1038/nature03074; Received 30 August 2004; Accepted 1 October 2004

Realization of quantum error correction

J. Chiaverini[1], D. Leibfried[1], T. Schaetz[1,3], M. D. Barrett[1,3], R. B. Blakestad[1], J. Britton[1], W. M. Itano[1], J. D. Jost[1], E. Knill[2], C. Langer[1], R. Ozeri[1] & D. J. Wineland[1]

1. Time and Frequency Division, Mathematical and Computational Sciences Division, NIST, Boulder, Colorado 80305, USA
2. Mathematical and Computational Sciences Division, NIST, Boulder, Colorado 80305, USA
3. Present addresses: Max Planck Institut für Quantenoptik, Garching, Germany (T.S.); Physics Department, University of Otago, Dunedin, New Zealand (M.D.B.)

Correspondence to: J. Chiaverini[1] Email: john.chiaverini@boulder.nist.gov

Scalable quantum computation[1] and communication require error control to protect quantum information against unavoidable noise. Quantum error correction[2, 3] protects information stored in two-level quantum systems (qubits) by rectifying errors with operations conditioned on the measurement outcomes. Error-correction protocols have been implemented in nuclear magnetic resonance experiments[4, 5,

Top

subscribe to nature

FULL TEXT
- Previous | Next
- Table of contents

Download PDF
Send to a friend
Scopus lists 79 articles citing this article
Export citation
Export references
Rights and permissions

Will QIP Become Practically Significant?

Phys. Rev. A 78, 062307 (2008): Experimental quantum secret sharing using telecommunication fiber

http://pra.aps.org/abstract/PRA/v78/i6/e062307

Physical Review A
atomic, molecular, and optical physics

American Physical Society APS physics

Log in | Create Account (what's this?)
RSS Feeds | Email Alerts

Home Browse Search Subscriptions Help

Citation Search: Phys. Rev. Lett. Vol. Page/Article Go

Your access to this article is provided through the subscription of Glasgow University Library

APS » Journals » Phys. Rev. A » Volume 78 » Issue 6

< Previous Article | Next Article >

Phys. Rev. A 78, 062307 (2008) [6 pages]

Experimental quantum secret sharing using telecommunication fiber

Abstract | References | No Citing Articles

Download: PDF (153 kB) Export: BibTeX or EndNote (RIS)

Jan Bogdanski, Nima Rafiei, and Mohamed Bourennane
Physics Department, Stockholm University, SE-10691 Stockholm, Sweden

Received 12 May 2008; revised 25 October 2008; published 4 December 2008

We report quantum secret sharing experiment in telecommunication fiber in five-party implementation. The quantum secret sharing experiment has been based on a single qubit protocol, which has opened the door to practical secret sharing implementation over fiber channels and in free space. The previous quantum secret sharing proposals were based on multiparticle entangled states, difficult in the practical implementation and not scalable. The secret sharing protocol has been implemented in an interferometric fiber optics setup with phase encoding and demonstrated for three, four, and five parties. The experimental setup measurements have shown feasibility and scalability of secure multiparty quantum communication over commercial telecom fiber networks.

University of Glasgow

Will QIP Become Practically Significant?

Most researchers are not convinced that D-Wave has built a quantum computer.

Will QIP Become Practically Significant?

Quantum cryptography is already practical. Whether there is real demand for it remains to be seen.

Quantum computing seems feasible in principle, although there are formidable scientific and engineering problems.

> **Decoherence: loss of quantum state due to unwanted interaction with the environment.**

BUT remember that in 1949, the statement "In the future, computers may weigh no more than 1.5 tonnes" was a speculative prediction.

Why Consider Formal Methods?

There is no doubt about the correctness of quantum algorithms and protocols.

Teleportation can be checked with a few lines of algebra.

Shor's and Grover's algorithms have been thoroughly studied.

Mayers (2001) and others have proved the security of quantum cryptography.

But what about systems – combinations of classical and quantum communication and computation?

University of Glasgow

Why Consider Formal Methods?

Raja Nagarajan and I (2002) suggested applying formal methods to quantum systems, with the same motivation as for classical systems:

Formal modelling languages, for unambiguous definitions.

Analysis of systems, rather than idealized situations.

Systematic verification methodology, rather than ad hoc reasoning.

Tool support.

I have been working on the following strands:

Process calculus for quantum systems
(with Raja Nagarajan and Tim Davidson)

Model-checking for quantum systems
(with Raja Nagarajan and Nick Papanikolaou)

Formal description of physics experiments
(with Sonja Franke-Arnold and Ittoop Vergheese Puthoor)

For the rest of this talk, I will focus on process calculus.

A protocol for transferring an unknown quantum state from Alice to Bob, making use of classical communication and some pre-existing shared entanglement.

$$x, y = |00\rangle + |11\rangle$$

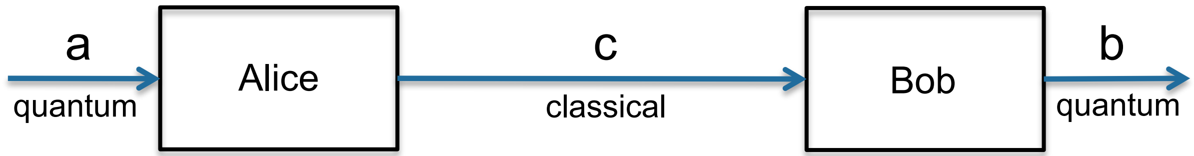
Alice		Bob
x		y
unknown u		
apply CNot to u,x		
apply H to x	Alice sends 2-bit classical result r to Bob	y has the initial state of u, up to an isomorphism determined by r
measure u,x	$\longrightarrow$	

We have developed the process calculus Communicating Quantum Processes (CQP) for modelling combined quantum/classical systems (SG + Nagarajan, 2005, 2006).

CQP has a formal syntax, a formal operational semantics, and a type system.

(Other approaches: QPAlg (Jorrand+Lalire 2004), qCCS (Ying et al. 2006-2011))

Quantum Teleportation in CQP



Alice(q,in,out) = in?[u] . { u,q *= CNot } . { u *= H } . out![measure u,q] . Stop

Bob(q,in,out) = in?[r] . { q *= Pauli$_r$ } . out![q] . Stop

Teleport(a,b) = (qbit x, y)({ x *= H } . { x,y *= CNot } .
(new c)(Alice(x,a,c) | Bob(y,c,b)))

creates the entangled pair

Running the Teleportation Protocol

A configuration consists of a quantum state and a process.

The semantics of CQP specifies transitions between configurations.

Each transition is a communication or an operation on the quantum state.

w = α|0〉+β|1〉 ; a![w] . Stop | Teleport(a,b) | b?[v] . Stop

=

w = α|0〉+β|1〉 ; a![w] . Stop | (qbit x, y)({ x *= H } . { x,y *= CNot } .
(new c)(Alice(x,a,c) | Bob(y,c,b)))
| b?[v] . Stop

Running the Teleportation Protocol

w,x,y = (α|0〉+β|1〉)|00〉 ;

a![w] . Stop | { x *= H } . { x,y *= CNot } . (new c)(Alice(x,a,c) | Bob(y,c,b))
| b?[v] . Stop

↓

w,x,y = (α|0〉+β|1〉)(|00〉+|11〉) ;

a![w] . Stop | (new c)(Alice(x,a,c) | Bob(y,c,b)) | b?[v] . Stop

=

w,x,y = (α|0〉+β|1〉)(|00〉+|11〉) ;

a![w] . Stop | a?[u] . { u,x *= CNot } . { u *= H } . c![measure u,x] . Stop
| Bob(y,c,b)
| b?[v] . Stop

Running the Teleportation Protocol

$w,x,y = (\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|11\rangle)$;

{ w,x *= CNot } . { w *= H } . c![measure w,x] . Stop | Bob(y,c,b) | b?[v] . Stop

$\downarrow$

$w,x,y = \alpha(|000\rangle+|011\rangle+|100\rangle+|111\rangle)+\beta(|001\rangle+|010\rangle-|101\rangle-|110\rangle)$;

c![measure w,x] . Stop | Bob(y,c,b) | b?[v] . Stop

$\downarrow$

¼•($w,x,y = \alpha|000\rangle+\beta|001\rangle$; c![0] . Stop | Bob(y,c,b) | b?[v] . Stop)
\+ ¼•($w,x,y = \alpha|011\rangle+\beta|010\rangle$; c![1] . Stop | Bob(y,c,b) | b?[v] . Stop)
\+ ¼•($w,x,y = \alpha|100\rangle-\beta|101\rangle$; c![2] . Stop | Bob(y,c,b) | b?[v] . Stop)
\+ ¼•($w,x,y = \alpha|111\rangle-\beta|110\rangle$; c![3] . Stop | Bob(y,c,b) | b?[v] . Stop)

$\downarrow$ ¼

Running the Teleportation Protocol

$w,x,y = \alpha|011\rangle+\beta|010\rangle$; c![1] . Stop | Bob(y,c,b) | b?[v] . Stop

=

$w,x,y = \alpha|011\rangle+\beta|010\rangle$;

c![1] . Stop | c?[r] . { y *= Pauli_r } . b![y] . Stop | b?[v] . Stop

$\downarrow$

$w,x,y = \alpha|011\rangle+\beta|010\rangle$; { y *= Pauli_1 } . b![y] . Stop | b?[v] . Stop

$\downarrow$

$w,x,y = \alpha|010\rangle+\beta|011\rangle$; b![y] . Stop | b?[v] . Stop

=

$w,x,y = |01\rangle(\alpha|0\rangle+\beta|1\rangle)$; b![y] . Stop | b?[v] . Stop

Specifying Correctness of Teleportation

We defined Teleport(a,b)**, which receives a qubit on channel** a **and sends a qubit on channel** b**, using teleportation in between.**

The following process has the same effect, and we regard it as a specification of teleportation.

Identity(a,b) = a?[x] . b![x] . Stop

Now we want to state the requirement that

Teleport(a,b) ≈ Identity(a,b)

and prove that it is satisfied. So we need a theory that defines ≈ and provides some proof techniques.

Behavioural Equivalence

The relation ≈ is a behavioural equivalence: if P ≈ Q then P and Q have indistinguishable behaviour.

It is a form of probabilistic branching bisimulation, where the observations take into account the amount of information that a transition reveals about the quantum state.
(Matching of transitions considers the reduced density matrix w.r.t. input/output qubits).

The aspiration for behavioural equivalence is congruence:

$$P \approx Q \implies C[P] \approx C[Q]$$

for all process contexts C. This supports equational reasoning. Congruence properties are sometimes known as composability properties.

Congruence for CQP

Obtaining a congruence relation for a quantum process calculus was an open problem for a while.

We have solved it for CQP (Tim Davidson's PhD thesis, 2011) and Ying et al. have independently solved it for qCCS (POPL 2011). **(The details are quite complicated and require changes to the semantics).**

We can show that Teleport(a,b) ≈ Identity(a,b)
and therefore this equivalence holds in all contexts.

Although correctness of teleportation is standard, this formulation is (we claim!) a valuable new perspective.

Mixed Configurations

A mixed quantum state is a probability distribution over pure quantum states, representing classical uncertainty.

We introduce mixed CQP configurations, distinct from probabilistic configurations. A measurement produces a mixed configuration. If the measurement result is output then a probabilistic configuration is produced.

Internal communication of a measurement result, however, does not remove mixedness.

In teleportation, with this new semantics, there are no probabilistic configurations, because the measurement result is never output.

No Mixed Configurations => No Congruence

Consider P = a?[x] . {measure x} . Stop
Q = a?[x] . {x *= H} . {measure x}. Stop

They are equivalent, in all quantum states, just because they produce no output.

Put them in parallel with R = b![q] . Stop

in the state p,q = |00〉+|11〉 .

If the measurement produces a probabilistic configuration, and R **outputs afterwards, then the possible reduced density matrices for** q**, produced by** P | R **and** Q | R**, are different.**

This means that P | R **and** Q | R **do not have matching output transitions.**

Mixed Configurations => Congruence

Consider P = a?[x] . {measure x} . Stop
Q = a?[x] . {x *= H} . {measure x}. Stop

They are equivalent, in all quantum states, just because they produce no output.

Put them in parallel with R = b![q] . Stop

in the state p,q = |00〉+|11〉 .

In the modified semantics, the measurement produces a mixed configuration and because the result is not output, it never becomes a probabilistic configuration.

Then the output of q **has the same reduced density matrix for both** P | R **and** Q | R **.**

Next Steps for Quantum Process Calculus

To make reasoning about processes easier and more practical:

- **equational axiomatization of equivalence**

- **automated equivalence checking**

More substantial applications, e.g. cryptography.

Conclusion

Quantum information processing is a fascinating research area which might lead to important computational and cryptographic technologies.

In any case, seeking to understand the computational power of quantum systems is a basic research question that approaches fundamental physics from an interesting new angle.

The formal methods approach, and process calculus in particular, will be needed for assurance of practical systems, and gives an interesting new perspective on quantum behaviour.