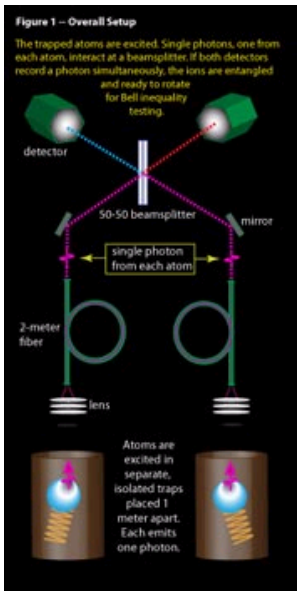
News archive

- 2010
  - April 2010
  - March 2010
  - February 2010
  - January 2010
- 2009
- 2008
- 2007
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001
- 2000
- 1999
- 1998
- 1997

Randomness is no lottery thanks to entangled ions

Apr 14, 2010 2 comments

An international team of physicists has created the first system that can produce verifiably random numbers. The technique relies on the inherent uncertainties in quantum mechanics and future versions could help cryptographers to encode information more securely than ever before.



Rolling quantum dice

Randomness is central to modern cryptography, which uses long strings of random numbers to form "keys" that can encode and decode sensitive information. Normally such strings are churned out by complex mathematical algorithms, called pseudo random-number generators. But these only approximate random strings, and there is the constant worry that hackers could somehow predict the sequences and gain access to secret files.

Worse still, cryptographers can never be sure that a pseudo random-number generator is unique and genuine. There is no way to prove a string is truly random, and even if it is, there is no way to know if a copy exists elsewhere. "If somebody gives you a bunch of numbers and claims they are random you should be suspicious," says Christopher Monroe, a physicist at the University of Maryland, US, and leader of the experimental group.

Impossible to copy

Monroe's group, which has worked alongside physicists at the Université Libre de Bruxelles in Belgium, the Institute of Photonic Sciences in Spain and Cambridge University in the UK, has used quantum mechanics to produce random strings that are impossible to copy. In the quantum world, an object exists in a mixed-up superposition of states until it is measured, at which point it collapses randomly into one of them. In principle, therefore, by observing a sequence of superposed objects, one can generate a sequence of random results.

To do this experimentally, Monroe's team employed a method known as a Bell test, named after the late physicist John Bell who invented it in 1964. They placed two atomic ions in separate enclosures one metre apart, and then "entangled" them by passing single photons through them. Once entangled, the state of one atom is inextricably linked to the superposed state of the other, so that a measurement of one – in this case, a measurement made by recording the emission of light – causes the states of both atoms to collapse.

Over the course of a month, the researchers measured the states of more than 3000 entangled atomic ion pairs, generating a string of 42

Related stories

Combing makes for neat qubits
Worldwide quantum security
Quantum encryption sets speed record
Key to the quantum industry (in depth)
A quantum renaissance (in depth)

Related links

Christopher Monroe

Restricted links

Nature **464** 1021

binary digits. Because the correlations between the measured states were less than a certain value, as given by Bell's famous "inequality", they were – according to quantum mechanics – certifiably random.

Perfect detection

Bell tests have been performed many times before, however. In particular, they have been performed to show that entanglement can affect the state of objects instantly, even if they are far enough apart that no signals could travel between them without breaking the speed of light – and Einstein's theory of special relativity. What makes Monroe's experiment different is that every entanglement event is recorded. In past attempts, limitations in detector efficiency have allowed many state collapses to pass by unnoticed. "Our system of trapped atomic ions separated in space with perfect detection is the only system that can be used for this purpose," says Monroe.

Our system of trapped atomic ions separated in space with perfect detection is the only system that can be used for this purpose

Christopher Monroe, University of Maryland

The researchers are now looking to improve the speed of random-number generation by increasing the efficiency of entanglement, perhaps embedding the system in a solid-state chip.

The research is published in *Nature* **464** 1021.

About the author

Jon Cartwright is a freelance journalist based in Bristol, UK

2 comments

Add your comments on this article

1 **leonardo.motta**
Apr 15, 2010 5:54 AM
Hanover, United States

<quote>An international team of physicists has created the first system that can produce verifiably random numbers. </quote>

This seems an odd claim. Thus far any quantum system is truly random and that can be verified. One example would be to watch beta decay and get a string of numbers out of that. There is nothing special about doing this so I do not understand what is the true breakthrough here. Moreover, there is even a company out there that claims it has a pocket quantum system that is a true random number generator:

www.idquantique.com…oducts-overview.html

Also, cf. arxiv.org…1004.1521

Edited by leonardo.motta on Apr 15, 2010 5:57 AM.

Reply to this comment · Offensive? Unsuitable? Notify Editor

2 **owengithua**
Apr 15, 2010 7:02 AM

a random number is random, that suits it.

Quote:

> *Originally posted by* ***leonardo.motta***
> <quote>An international team of physicists has created the first system that can produce verifiably random numbers. </quote>
>
> This seems an odd claim. Thus far any quantum system is truly random and that can be verified. One example would be to watch beta decay and get a string of numbers out of that. There is nothing special about doing this so I do not understand what is the true breakthrough here. Moreover, there is even a company out there that claims it has a pocket quantum system that is a true random number generator:
>
> www.idquantique.com…oducts-overview.html
>
> Also, cf. arxiv.org…1004.1521

Reply to this comment · Offensive? Unsuitable? Notify Editor