appeared on 17th Sep 2009

Quantum computers cast shade on e-commerce

The infant quantum computer has taken her first steps, says S.Ananthanarayanan.

In quantum mechanics, which is the version of the laws of motion that are valid at very small dimensions, an entity that can take different states of existence is not in one of these states at any instant, but in all of them, so long as no measurement is made of its state. For example, if an electron can exist in a state of 'spin up' or 'spin down', its normal state is not one of the two states, but both the states, with a given probability that it will be found in one state or the other if the state is measured.

This is a basic departure from our usual understanding of things, and this way of looking at nature, along with other concepts, like the particle nature of waves and the principle of uncertainty, which is the limit to how accurately both the position and the speed of a particle, or the energy of a state and the time for which it will last, can be measured, is the only way that many realities of nature, like radioactivity, the photo-electric effect, atomic structure and so on, can be explained.

A consequence, or it may be a requirement, of this nature of small things is also that the state of a thing, so long as it is not disturbed by a measurement, must be in all the possible states that it is capable of being in, all at the same time. A collection of such objects then can be programmed to make a calculation where different possible values of a set of variables are considered at the same time and calculations made in a fraction of the time they would normally take.

Independent research groups, one led by Andrew White in Brisbane, Australia and another led by Chao-Yang Lu in China, and also Jeremy O'Bbien and colleagues in Bristol,UK, have built devices that are able to do rudimentary calculations in this way. The development is seen as promising of more complex arrangements to carry out computations that are not even conceivable with traditional devices.

RSA Code

The world of e-commerce depends on transactions being coded with the help of a pair of numbers, known only to the sender of a message, and stored in such a way that the numbers cannot be deduced by an outsider. This code then helps protect the authenticity of the message of a sender, or the secrecy of a message to be opened by only the person who has the code.

One method, called the RSA code after the names, Rivest, Shamir and Aldeman, of its inventors, is that a number called the 'public key', is the product of two very large prime numbers. The key then has only two unique divisors on which is based the private key. A message coded with the help of the private key, then, can be opened with the help of the public key, which is freely available, but only if it had been coded by the private key. Conversely, a message coded with the public key can only be opened with the use of the private key.

appeared on 17th Sep 2009

Cracking the code is difficult because, if large prime numbers are used to generate the product, it would take too long to work out the two unique prime numbers which are its only divisors. With a product that has ten digits, for example, about 100,000 trials need be made to detect the divisors. A fast computer can do this in a trice. But if the number is 50 digits long, then, it takes about 10 trillion trillion trials and a computer would take a century!

Actual public keys use many more than 50digits and the codes are secure indeed.

Enter quantum computer

The reason the computation takes so long is that a solution needs to be found by trying out all possibilities one after another, that is, sequentially. Even if there were a data base of all the primes lower than say the square root of an 80 digit number, there are too many of such primes and trying to divide the number by each of the primes, till a solution is found, would take years and years.

A solution may thus lie in doing the computations not one after another but all at the same time. This is easier said than done. Some 15 years ago, a computer scientist called ***Peter Shor*** devised an algorithm for a computer with components which could take more than one state at a time to carry out this calculation. It was a brilliant solution, but only a drawing board one, because such a computer was only the quantum computer and this had not been actualized!

In such a computer, in its simple form, each component could take the value of ‘0’ or’’1’, and in the normal state, would be in a combined state of both '0’ and ‘1’. Two such components, would thus represent the binary numbers, ‘00’, ‘01’, ‘10’ and ‘11’, all at the same time. These numbers represent the numbers 0,1,2,3, in ordinary numbers. If there were another such pair of components, and an arrangement to evaluate the product were devised, the product would ‘0,1,2,3,4 , 6 and 9’, all at the same time. If there was a filter for ‘9’, the numbers ‘3 and 3’ could then be separated, or if the filter was for 4, the numbers ‘2 and2’

The interesting thing is that the pair, ‘3,3’ or ‘2,2’ would be determined in a single computation, without having to try out all the possible combinations separately. It is easy to see that with a large number of such components, very large computations can also be carried out, in the same way, in a single ‘visit to the table’.

Real computers

Real quantum computing was first done in 2001 by IBM engineers who used nuclear magnetic resonance, a technique that is useful in medicine, to track the way molecules of fluorocarbon interacted. This proved the possibility, but had no promise for practical use because filtering and measurements are not possible with more than just a few molecules.

appeared on 17th Sep 2009

The Brisbane, China and Bristol teams used a laser to generate photons which they passed through specific crystals, to created pairs which were in a combination of the 2x2=4 states of a pair of photons. Using such photon pairs and optical filters to select particular photon spins, they were able to simulate Shor's algorithm and evaluate the prime factors, 3 and 5, of the number 15.

It is only a 'baby step' towards the quantum computer, but it shows that a large scale arrangement, both to crack computer codes as well as to solve real problems that are too complex for ordinary computers, is feasible.

In the meantime, code-makers have got busy to generate codes that quantum computers cannot break, to keep the other side of commerce alive and thriving.