Lab Rat: Actually, this is rocket science

on 13 September 2000, 22:00 listen now

by Niall McKay

To get this column sent to your inbox, subscribe to the email newsletter.
We've got a problem. Moore's Law -- the tenet that says the number of transistors (and therefore the performance) on a microprocessor doubles every 18 months -- will run out of steam around 2012.

By then, transistors will be about three atoms thick. So what will we do to drive performance forward? The solution, some of the world's most eminent computer scientists believe, is an obscure branch of science called quantum physics.

University, government, and corporate research labs, such as Stanford, the Department of Energy's Los Alamos National Labs, the National Institute of Standards and Technology, IBM, AT & T Labs, Lucent's Bell Labs, NASA's Ames Research Center, Hewlett-Packard, and even Microsoft, are currently investing heavily in quantum computing.

Now, before you go on a rampage with your 401k savings plan looking for quantum startups (I know of only one, MagiQ Technologies), understand that this is a long way from being cooked.

SHOR THING

In fact, until six years ago, when Peter Shor, a scientist at AT & T Labs, invented a quantum factorization algorithm, it was little more than a passing curiosity for propeller heads.

Dr. Shor's algorithm, together with a quantum computer, is a very powerful thing. For instance, it makes nonsense of cryptography because, in theory at least, it can factorize large numbers very quickly (factoring presents major difficulties for current technology). One bit in a standard computer is represented by a single digit that is either 0 or 1. But a quantum bit, or qubit, can be represented by an atom or photon and can exist simultaneously as 0 and 1 or anything in between. This means that it can calculate many possibilities simultaneously -- it's a massive parallel computing system, if you will. So, there are tasks that even a crude quantum computer can do that are nearly impossible for a classical computer.

LOV'S LABOR NOT LOST

Factorization is all very well for those who hate encryption, like the National Security Agency, but who else wants a quantum computer? Lov Grover of Bell Labs came up with a variation that would make them very useful because they can search a database very rapidly.

"No one really uses their computers for factorization, but searching is something we could do a lot more efficiently," Dr. Grover says.

He recently improved on his work and now if you know only a first name and, say, a street number of a person in the New York metropolitan area, it'll find them in a jiffy. For example, a list containing 10,000 items would take a current computer 5,000 steps, compared with only 100 steps using a quantum computer and the Grover algorithm.

ROCKET SCIENCE

Meanwhile, rocket scientist Deepak Srivestava at NASA's Ames Research Center believes that a modified version of Grover's algorithm can be used for space exploration.

"Our interest is to create computer simulations of planets and then mine this data to do predictive modeling," he says. "We would use this data to do planetary exploration."

However, there is a problem. Quantum computer hardware, so to speak (because it's usually liquid), is not quite ready yet. There are basically two types of quantum computers in development: a Nuclear Magnetic Resonance (NMR) computer, pioneered by Dr. Richard Hughes and his team at the Department of Energy's Los Alamos National Labs in New Mexico just 20 months ago, and the ion trap computer, which was developed by physicist David Wineland of the National Institute for Standards and Technology. Los Alamos's quantum computer had just three qubits, but since then IBM's Isaac Chuang has come up with a five-qubit quantum computer, and then in May, Los Alamos brought out a seven-qubit quantum computer.

All, however, have their limitations, owing to the fact that if you touch, tamper with, or even look at a qubit you have distorted the results. This makes it difficult to program. Scientists are compelled to use the NMR machine to nudge chloroform

RED HERRING'S BLOG

Strolling Along to a Different iTune
Can Amie Street break Apple's download dominance?

HIT: Where Healthcare Meets Tech
The buzz surrounding healthcare IT provider, Cerner

Listen Up
Able Planet's new headset offers up solid aural vibes.

Gmail BETA, See You Lata
Google's gmail loses its "BETA" label.

Bada Bing, Bada Boom?
Microsoft's Bing.com gets some traction in online search, according to the numbers in from ComScore.

Calpers to Pump up PE Stake
The nation's largest pension fund is mulling a 40 percent increase in its private equity investments.

Peripheral Madness
The living room is a jungle of plastic and wires – I say enough already.

Wii Storage Ups Strong Bad Sales
One company is feeling the love because of Nintendo's Wii storage solution: Telltale's Strong Bad.

Amazon Sells Xbox Live Games
No more leftover points–buy XBLA games off Amazon.

GDC 09 Keynote: What About Wii?
Satoru Itawa's keynote touched on both systems, but it seems like the Wii got the short end of the stick.

Steam Vaporizes DRM and Piracy
Steam's added anti-piracy measure does away with DRM.

FINANCE
Allegis' Ackerman: U.S. Innovation 'Stalling'
AT&T Unleashes MMS for iPhone
A123 IPO Juices 40 Percent

INTERNET
Allegis' Ackerman: U.S. Innovation 'Stalling'
Rubicon to Buy Others Online
Intuit Takes Mint.com for $170M

CLEANTECH
A123 IPO Juices 40 Percent
Index Ventures: Envy of Industry
Accel: No. 1

MEDIA
Allegis' Ackerman: U.S. Innovation 'Stalling'
Top 100 Global Venture Capitalists
HP's Earning Fall 19 Percent

COMPUTERS
Allegis' Ackerman: U.S. Innovation 'Stalling'
AT&T Unleashes MMS for iPhone
A123 IPO Juices 40 Percent

COMMUNICATIONS
Allegis' Ackerman: U.S. Innovation 'Stalling'
A123 IPO Juices 40 Percent
Rubicon to Buy Others Online

BIOSCIENCES
Index Ventures: Envy of Industry
Accel: No. 1
Medsphere Injected With $12 Million

SECURITY
Top 100 Global Venture Capitalists
HP's Earning Fall 19 Percent
Cisco Engulfs Tidal Software for $105M