Lab Rat: Actually, this is rocket science, part 2

on 20 September 2000, 22:00 listen now

by Niall McKay

In the quantum computing community, IBM research scientist Nabil Amer is an odd fish. While most scientists are frustrated by the fact that if you touch, tamper with, or even look at the atoms in a quantum computer, you distort the results, he embraces the principle. That's because he is depending on it to create a new type of tamper-proof security technology called quantum encryption.

"Anybody looking at or copying a quantum stream of information will automatically corrupt the data," says Mr. Amer. "This renders the information useless and alerts the recipient that there is something wrong."

Mr. Amer's quantum encryption team has made significant progress in the past 12 months and estimates that they will have a working prototype of an encryption engine in the next two years.

IBM is not the only company investing in the technology. The Department of Energy's Los Alamos National Labs, Toshiba, British Telecom, and Japan's NTT are also developing quantum encryption techniques.

Over at Los Alamos, quantum information team leader Richard Hughes is running a quantum encryption program to develop the technology for the military and satellite communities.

ENGAGE OR EMBRACE

"You can either fight quantum or embrace it," Mr. Hughes says. "But we believe that it will provide the security that the military requires, because to break current cryptography is a question of mathematical difficulty, but to break quantum encryption, you've got to break the laws of physics."

Still, it would be a mistake to believe that quantum computing will change our world in the near term. For one thing, experts including Mr. Amer and Mr. Hughes say that it will be at least 20 years before we have a commercial version of a quantum computer. And then it will only be good at certain applications such as database searching.

Bell Lab's Lov Grover spends most of his time trying to dream up applications for quantum computing. "They will be very good at doing massively parallel computation," he says. "But we are still looking for other useful applications."

"Perhaps speech synthesis or artificial intelligence," Mr. Grover ventures. "But not even a quantum computer can crack computing's greatest conundrum -- the traveling salesman problem. If you have a salesman that needs to travel between a dozen cities, how do you calculate the shortest route?

"It's easy when the number of destinations is low," continues Mr. Grover. "But what if you are trying to route bits across the Internet, where there are possibly millions of locations?" That is the problem that Mr. Grover is working with quantum computing to try to solve.

SILICON SPIN

The length of time until quantum computers can be practically applied also has researchers like Mr. Amer raising questions. He's in the minority, but he believes that, until now, we have been perhaps going down the wrong road by developing Nuclear Magnetic Resonance (NMR) and ion trap quantum computers.

"We've made great progress with NMR quantum computers; however, it's a completely new branch of science," he says. "I believe that we should leverage the current trillion-dollar silicon industry to develop a solid-state quantum computer."

Mr. Amer believes that super-conductivity -- that is, getting an electron to move down a piece of wire without producing any heat -- is the way to make quantum computers solid state. That way qubits could be free to calculate without being modified by their environment.

And that's probably the way that this industry will go. For instance, Hewlett-Packard's interest in quantum computing is in order to reduce the size of today's computers, rather than to develop a new branch of science.

"We are nearing the stage where transistors are so small that they are governed by the laws of quantum physics anyway," says Deepak Srivestava of NASA's Ames Research Center. "We are focusing on doping silicon-based materials rather than using NMR quantum computers."

SEARCH

Google Search

GOOGLE TRANSLATIONS FOR RED HERRING

CHI FRA GER HEB ITA JAP KOR RUS SPA

RED HERRING'S GLOBAL VC 100

The Global 100 VC Winners
For the first time and after many weeks of evaluation, Red Herring is proud to announce the following 100 VC firms from around the Globe have won the 2009 Global VC 100. **Click here** to find out who the lucky winners are.

The World's Top VCs
Red Herring is busy searching for the top 100 global venture capital firms. The 200 finalists have been announced. Please **click here** to see the best 200 performers from over 30 nations.

RED HERRING 100 EVENTS

Red Herring 100 Europe, Berlin, Germany
The Red Herring 100 is a mark of distinction and prestige. Only 200 companies are chosen as finalists from across Europe. The 100 Winners have been announced. Click here to see the lucky winners.

Red Herring 100 N. America, San Diego, CA
The Red Herring 100 is a mark of distinction and prestige. Only 200 companies were been chosen as finalists from a pool of thousands. The 100 Winners were announced at the award ceremony. **Click here** to see all the winners.

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