Harnessing the power of quantum computing: Early stages: There's a huge gulf between what quantum computers can do in theory and what they can do in practice.

The Ottawa Citizen

June 10, 1997, Tuesday, FINAL EDITION

Copyright 1997 CanWest Interactive, a division of CanWest Global Communications Corp. All Rights Reserved

Section: BUSINESS; Pg. C6

Length: 775 words

Byline: TOM STANDAGE; THE DAILY TELEGRAPH

Dateline: LONDON

Body

What will the computers of the future be like? In the short term, it's not too hard to predict: if current trends continue, the high-end desktop PC of 2007 will probably have four 999MHz processors, 512Mb of RAM, and 2,000 gigabytes of storage.

But what about the long term?

According to some researchers, far more powerful computers could be built by firing laser beams at trapped atoms, or radio pulses into a cup of hot coffee. Those are just two techniques doing the rounds in the bizarre field of quantum computing. Researchers gathered in London last month to discuss the latest developments in what has become one of the most extraordinary areas of computer research.

The idea of quantum computing was first put forward by Nobel prize-winning physicist Richard Feynman in 1982, but was purely a matter of theoretical interest until 1994 when Peter Shor, a researcher at Bell Laboratories, showed that a quantum computer could crack codes far faster than conventional machines. For example, that year it took 1,600 workstation computers eight months to factorize a 129-digit number -- the kind of difficult operation that is relied upon to ensure the security of modern cryptography.

At that rate, factorizing a 1,000-digit number would take 10 million billion billion years -- billions of times longer than the age of the universe. But Mr. Shor's work predicted that a relatively simple quantum computer could do it in about 20 minutes.

Suddenly, quantum computing was a hot topic -- because if a quantum computer could be built, it would turn the world of computing (not to mention cryptography) on its head. But so far, the most complicated thing anyone has got a quantum computer to do is add one and one to get two.

There's a big difference between what the speeds quantum computers are capable of in theory and what they can do in practice.

Building a quantum computer is difficult because the very thing that makes it so powerful -- its reliance on bizarre subatomic goings-on governed by the laws of quantum mechanics -- also makes it very fragile and hard to control. Classical computers store values as binary digits (bits) that can be 0 or 1. Quantum bits (known as qubits) can represent both 0 and 1 simultaneously, so a single qubit can be involved in two calculations at once.

Two qubits can carry out four operations at once, three eight, and so on. The more qubits you have, the more of a speed-up due to "quantum parallelism" you get, leading to potentially mind-boggling performance.

But since qubits can exist only at a subatomic level, operating a quantum computer is fiendishly fiddly. One approach is to use individual atoms cooled to very low temperatures to store each qubit, and painstakingly targeted laser beams to manipulate them. Another approach uses nuclear magnetic resonance (NMR) techniques to manipulate atoms within a solution of organic molecules -- such as the caffeine molecules found in coffee. It was a simple quantum computer built along these lines that recently calculated one plus one.

Dr. David Deutsch, of the Clarendon Laboratory in Oxford, England, who first put quantum computing on a firm theoretical foundation, believes quantum computing is inevitable, as components on today's chips cannot get much smaller without running into quantum effects themselves.

But, he adds: "From the moment Newton's laws were discovered, it was known that in principle we could go to the moon. But it was 300 years before we did." Deutsch compares the current state of quantum computing to classical computing in 1948, when the transistor was invented.

"There were useful inventions that involved one transistor, like a radio," he says.

"Then there came applications that used six or 10 transistors, and it took 20 years before you could have thousands of transistors on a chip and make a useful computing device out of it.

"There are quantum mechanical devices short of a fully fledged quantum computer which are useful, and do things that are classically impossible."

He points out that quantum computing has already produced useful spin-offs, such as quantum cryptography ("something a classical computer cannot do") and more accurate atomic clocks.

"But what is important here is not the final destination but the journey," says his co-researcher, Artur Ekert. "Imagine if you'd gone into Charles Babbage's study in the 19th century and asked him what his computer was good for. He'd have said for tabulating logarithms -- he couldn't have imagined the Internet, or word processing, or games. With anything new you don't really know where it will take you."

Classification

Language: ENGLISH

Subject: QUANTUM COMPUTING (93%); COMPUTER SCIENCE (90%); QUANTUM MECHANICS (90%); TRENDS (89%); COMPUTATIONAL RESEARCH (76%); PHYSICS (76%); LASERS (73%); NOBEL PRIZES (73%); CRYPTOLOGY (71%); AWARDS & PRIZES (68%)

Company: BELL LABORATORIES (56%); BELL LABORATORIES (56%)

Industry: SIC3661 TELEPHONE & TELEGRAPH APPARATUS (56%); QUANTUM COMPUTING (93%); COMPUTER EQUIPMENT (90%); COMPUTER SCIENCE (90%); DESKTOP COMPUTERS (78%); PERSONAL COMPUTERS (78%); DATA STORAGE TECHNOLOGY (77%); COMPUTATIONAL RESEARCH (76%); LASERS (73%); CRYPTOLOGY (71%)

Geographic: LONDON, ENGLAND (74%)

Load-Date: June 11, 1997

End of Document