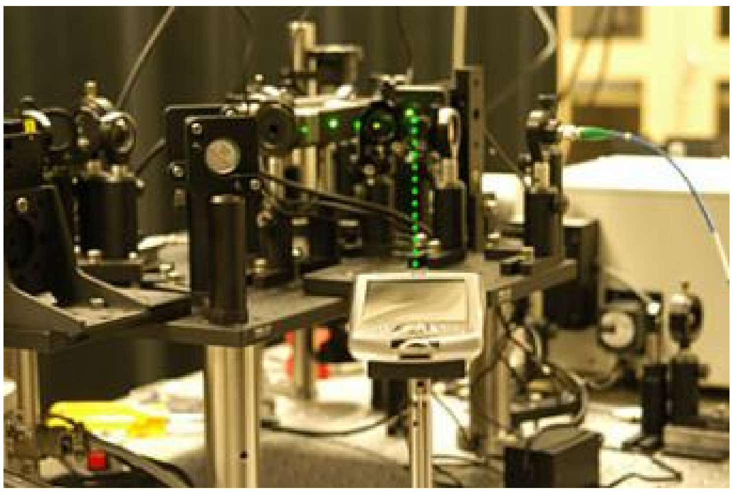
Scientific breakthrough a step toward quantum computing

January 3 2006



Light is the solution. It's also the problem. That's the paradox HP Labs' Quantum Information Processing Group is beginning to unravel with its research into optical quantum computing. The group has been investigating ways to use photons, or light particles, for information processing, rather than the electrons used in digital electronic computers today. Their work holds promise for someday developing faster, more powerful and more secure computer networks.

"Quantum processing can attack problems we can't attack with conventional computers," says Tim Spiller, the HP Distinguished

Scientist who is leading the research. "Even a small quantum computer has the potential to enhance communications and information processing."

Previous designs impractical

Today's computers work by manipulating bits that exist as either 0s or 1s. What makes quantum computing so powerful is that quantum bits (or qubits) have an infinite choice of values, meaning they can potentially perform multiple operations simultaneously. For example, a quantum computer could efficiently factor large numbers that today's, or even tomorrow's, conventional machines might never be able to crack.

Scientists have believed for years that high-speed light is the best candidate for moving quantum information from place to place. However, previous designs for quantum computing using light have been extremely inefficient, and so completely impractical for actual technology.

Challenges in working with light

"Light is very good for communication because the bits of lights don't talk to each other," Spiller explains. "You can send light over long distances — for instance, with optic fibers — and it preserves its state pretty well. It doesn't communicate with other bits of light — or with much else, either. That's why you can have many different conversations going on at the same time in the same telephone cable and they don't interfere with each other."

Therein lies the problem. "To do any kind of data processing, the bits of data need to be able to interact," as they do in today's computer systems, Spiller says. "So on the face of it, light isn't good for information processing because the bits of light don't talk to each other. We need a process to get pieces of light at the quantum level to talk to each other."

That's exactly what his team — including Principal Research Scientist Bill Munro, other HP Labs researchers and Kae Nemoto, an associate professor of quantum information sciences at the Tokyo-based National Institute of Informatics — has spent two years trying to develop.

Photon detection method a breakthrough

Their starting point was solving yet another puzzle: how to detect photons, or individual chunks of light, without absorbing or damaging them. Typically, detecting a single photon requires letting it "smack into" something, such as a piece of semiconductor material, Spiller says. "That creates a lot of electrons and holes, and the piece of light is lost. So you can detect it, but in the process of doing so, it's destroyed."

Now the team has developed a method for both detecting photons without appearing to harm them and for allowing the bits of light to communicate with each other by having the photons 'talk' with one another via a probe light signal. The photon leaves an imprint of itself on the probe light signal without being damaged in the process, allowing the researchers to detect it without apparently demolishing it.

"You can measure the probe light signal and look for the photon's imprint," Spiller explains. "If you see it, it's there; if you don't, it isn't."

Better communication, more security

Equally important: the probe light signal lets photons interact, albeit indirectly. "If you do a certain type of measurement on the probe after it's talked to two photons, you'll find that although they don't talk directly to each other, the photons have interacted because they both talk to the probe," Spiller says.

Theoretically, the researchers say, there's no limit to the number of photons that can interact this way. For that reason, their work represents a quantum step toward creating a scalable method for optical quantum computing.

"The nice thing about this is it's moving toward having the best of both worlds," Spiller says. "The best communication is done with light. If you can also compute with light, you can do everything with light." As a result, there is no need to convert quantum information from some type of electronic format to the new optical one and back.

Work to be done

The HP Quantum Information Research effort circles the globe, with researchers in Bristol, Palo Alto and Tokyo (Nemoto). Their efforts, which could fundamentally change the way computers and people work, have caught the attention of scientists worldwide. Many call the team's early findings important and promising, but warn that researchers are years away from being able to build a real optical quantum computing system.

Spiller readily concurs. "Our vision is long-term, and we're starting small," he says. We hope to have some experimental results in the next couple of years. Once we've got that started-once we know for sure how one photon can talk to one beam — we can go forward to build quantum processors."

Potential applications

Quantum computing has the potential to revolutionize information technology. Small quantum processors containing just a few qubits could be used to stretch out the distances over which secure quantum communications work, analogous to the way that conventional optical repeaters are used to amplify ordinary optical communications. Such small processors may also enable new sensing and measurement technology.

Comparably small (in terms of qubit number), but distributed, quantum processors could enable new protocols such as secure quantum auctions between separated parties, or quantum voting.

Mid-sized quantum processors (50-100 qubits) could be used as research tools, allowing simulation of quantum systems that currently cannot be performed on even the most powerful supercomputers. Large quantum computers (with tens of thousands of qubits) will likely be able to search more quickly than conventional technology and factor very large numbers efficiently, leading to quantum code-breaking.

New paradigm for IT

Other potential applications are likely to evolve over time. Munro points out that transistors were initially used in hearing aids.

"At that time, you only had big valves made of glass so you couldn't have a small integrated circuit. Then somebody put a few components on a small device used for hearing aids," he says. "The people who did that didn't foresee that down the road you'd have millions of transistors, or integrated circuits, on pieces of silicon, running devices of all types and sizes."

Spiller says he expects that quantum computing will enhance, rather than replace, the current standard.

"We believe quantum computing will grow alongside conventional computing. You might have a quantum processor sitting next to your conventional machine," he says. "It's not that quantum technology will sweep everything else away. Instead, it will enable new things."

Source: Hewlett-Packard (by Anne Stuart)