Researchers take step toward creating quantum computers using entangled photons in optical fibers

April 8 2008

For now, full-fledged quantum computers are the stuff of science fiction — in last summer's blockbuster movie Transformers, the bad guys use quantum computing to break into the U.S. Army's secure files in just 10 seconds flat.

But Prem Kumar, the AT&T Professor of Information Technology in the Department of Electrical Engineering and Computer Science and the director of the Center for Photonic Communication and Computing at Northwestern University's McCormick School of Engineering, and his research group are one step closer to realizing that technology — though for far better purposes. The group recently demonstrated one of the basic building blocks for distributed quantum computing using entangled photons generated in optical fibers, and their research was published in the April 4 edition of *Physical Review Letters*.

"Because it is done with fiber and the technology that is already globally deployed, we think that it is a significant step in harnessing the power of quantum computers," Kumar says.

Quantum computing differs from classical computing in that a classical computer works by processing "bits" that exist in two states, either one or zero. Quantum computing uses quantum bits, or qubits, which, in addition to being one or zero can also be in a "superposition," which is both one and zero simultaneously. This is possible because qubits are quantum units like atoms, ions, or photons that operate under the rules of quantum mechanics instead of classical mechanics.

The "superposition" state allows a quantum computer to process significantly more information than a classical computer and in a much shorter time.

The area of quantum computing took off about 14 years ago after mathematician/physicist Peter Shor created a quantum algorithm that could factor large integers much more efficiently than a classical computer. Such an algorithm put the computer world in a tizzy because many web sites secure information like credit card and bank account numbers over the Internet through the public-key cryptography method known as RSA, after its inventors Rivest, Shamir, and Adleman. This method is based on the assumption that it is computationally infeasible to factor very large integers on classical computers.

Though researchers are still many years away from creating a quantum computer capable of running the Shor algorithm, progress has been made. Kumar's group, which uses photons as qubits, found that they can entangle two indistinguishable photons together in an optical fiber very efficiently by using the fiber's inherent nonlinear response. They also found that no matter how far you separate the two photons in standard transmission fibers they remain entangled and are "mysteriously" connected to each other's quantum state.

For this paper, Kumar and his team used the fiber-generated indistinguishable photons to implement the most basic quantum computer task – a controlled-NOT gate, which allows two photonic qubits to interact.

"This device that we demonstrated in the lab is a two-qubit device — nowhere near what's needed for a quantum computer — so what can you do with it"" Kumar says. “It’s nice to demonstrate something useful to give a boost to the field, and there are some problems at hand that can be solved right now using what we have.”

The Defense Advanced Research Projects Agency has funded the group’s next effort to study how to implement a quantum network for physically demonstrating efficient public goods strategies, which are similar to the mechanism design theory that Nobel laureate Roger Myerson laid the foundation for while at Northwestern.

Kumar says such a network could help out with high stakes auctions, like if, for example, the Department of Defense wanted to build an expensive airplane and sends out a request for bids. No one company can build the entire airplane, and there could be 15 companies that can build some part of the airplane, whether it’s a navigation system or an engine.

But instead of just giving the project to the lowest bidder, the government could save public dollars by allowing these companies to bid in a complicated way that makes the process more efficient. Maybe the engine company has worked with the fuselage company before and, if they worked together again, could be more efficient and less expensive than another two companies working together. They could then send in a conditional set of bids, along with regular bids if the two companies were to work with other companies as well.

“Figuring out the best possible outcome is possible with quantum computers,” Kumar says. “Based on these fiber-type gates that we are building utilizing entanglement, the auctioneer has an efficient way of determining optimal outcomes when bidders make conditional bids. When the computation is done, it reveals only the winning strategy, and all other bids disappear.”

Kumar says they hope to perform this experiment sometime in the next year.

Source: Northwestern University