COMPUTERWORLD
FROM IDG
INSIDER EXCLUSIVE

Quantum computing advances toward the enterprise

It may still sound like science fiction, but quantum computing could be a reality within a decade

The stories in this package are:

- **Teleporting a photon leads researchers to quantum security**
- **IBM makes quantum computing available in the cloud**

Teleporting a photon leads researchers to quantum security

Canadian researchers go the distance - 3.5 miles, in this case

Sharon Gaudin | Computerworld

Come on, admit it. You've always wanted to have Scotty beam you up to the USS Enterprise.

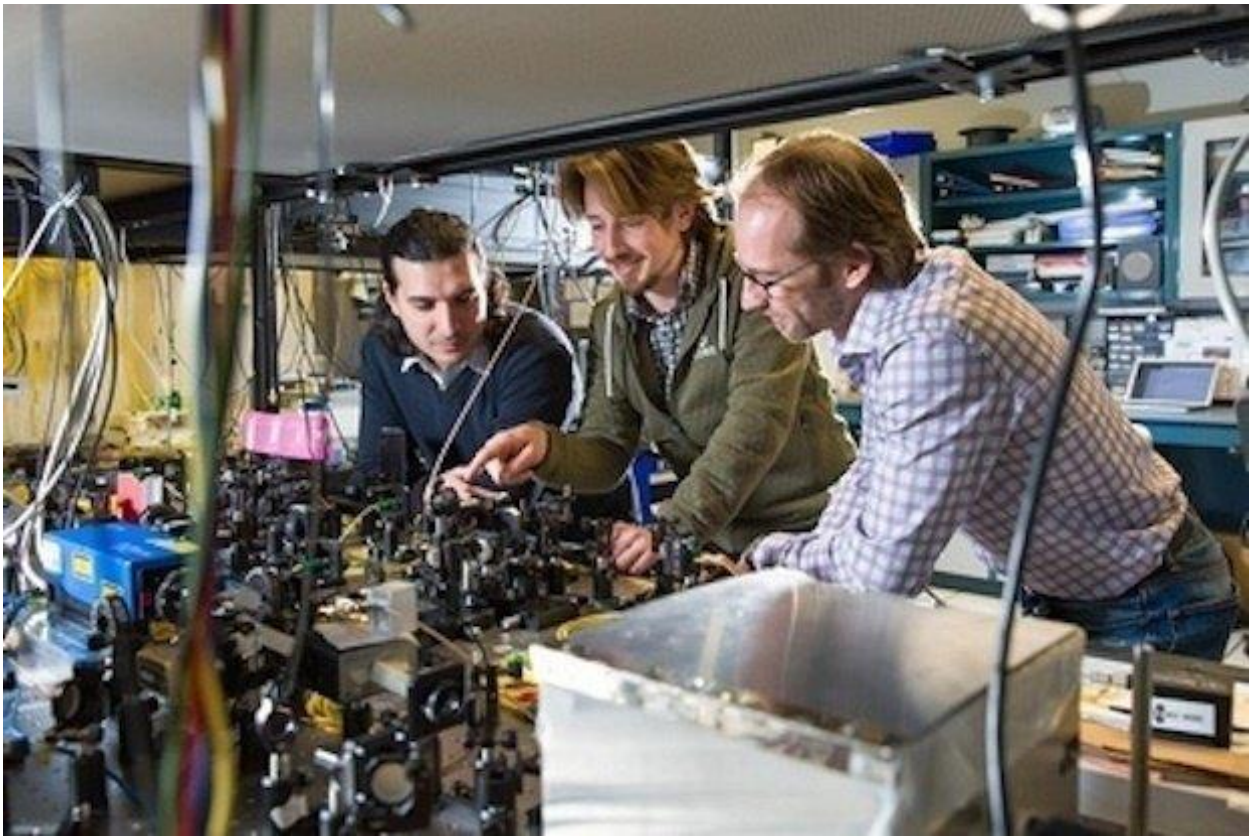
But it's unlikely that you will be teleported anywhere in this lifetime… unless you're a photon.

And that could mean more secure communications in the foreseeable future.

A group of physicists announced this week that they have successfully teleported a photon, which is a particle of light, over the span of just more than 3.5 miles in a straight length of fiber optic cable.

The effort, funded by the Defense Advanced Research Projects Agency, or DARPA, sets a world record for distance in quantum teleportation.

"Such a network will enable secure communication without having to worry about eavesdropping, and allow distant quantum computers to connect," said Wolfgang Tittel, in a statement. Tittel is a professor in the Department of Physics and Astronomy at the University of Calgary, where the research was done.



A group of physicists at the University of Calgary, including Wolfgang Tittel, right, a professor in the university's Department of Physics and Astronomy, have successfully teleported a photon over a distance of more than 3.5 miles.(Photo by Riley Brandt/University of Calgary)

The teleportation demonstration was conducted in the city of Calgary, using its fiber optic cable infrastructure.

Tittel said he's hopeful that we're only a little more than 10 years away from using quantum teleportation for online communications.

And that will be a very good thing for people interested in keeping their messages secure.

"What we need for secure communications over any channel is encryption," Tittel told *Computerworld* in an interview. "The way this is done today is based on mathematical algorithms. We believe that for a computer it takes thousands of years to decrypt this, but a

quantum computer would be able to decrypt these things much more rapidly -- like in seconds instead of thousands of years."

That means when quantum computers actually hit the market, which Tittel predicts will be in 10 to 20 years, our encrypted transmissions might not be so secure.

That's where quantum teleportation comes in.

With this technology, computers could imprint information or an encryption key on a photon, much like we print letters on paper, and then teleport it to the recipient.

The security piece: If someone tries to eavesdrop on that photon while it's being transmitted, the information on it automatically changes -- for both the eavesdropper and the intended recipient.

"It's a fundamental quantum law that we don't have in the traditional world of physics -- the no-copying theory," said Tittel. "In the quantum world, perfect copying is not possible. It means if you receive photons from me and you see the code keys have been changed, you can conclude that someone tried to steal information. If you see the key hasn't been changed, then nobody has tampered with the transmission."

This technology already exists today in a limited fashion.

The Geneva, Switzerland-based company ID Quantique offers quantum-safe crypto technology.

And a similar experiment about quantum encryption was recently conducted in China.

Today, though, the technology is restricted in terms of the distance that the quantum-secured information can be sent -- only about 62 miles.

"We could send secret keys inside the city but not much further," explained Tittel. "Not across Canada, for instance, and not between big cities."

In the future, no distance would be too far for quantum teleportation, he added.

Tittel's experiment was based on the theory of the entanglement property of quantum mechanics, which is a highly complex and mysterious branch of physics.

With entanglement, two objects, even if they are not physically connected or even close to each other, communicate and interact with each other.

"Being entangled means that the two photons that form an entangled pair have properties that are linked regardless of how far the two are separated," said Tittel, in the written statement. "When one of the photons was sent over to City Hall, it remained entangled with the photon that stayed at the University of Calgary."

Tittel explained that one other technology that needs to be advanced to create a true quantum network is quantum memory for light, which is much like a hard disk for quantum states.

Right now they exist only in laboratories.

"Our goal or next steps would be to improve quantum memory, quantum teleportation and then build a quantum network across Calgary and then across Edmonton and then across Alberta," said Tittel. "We'll have this way of communicating before we have readily available quantum computers that can easily break encryption."

So what about teleporting humans, instead of just photons? Are we close to the image we have in our heads from *Star Trek*?

The short answer, according to Tittel, is no.

IBM makes quantum computing available in the cloud

The company's 5-qubit processor is accessible on any desktop or mobile device

Sharon Gaudin | Computerworld

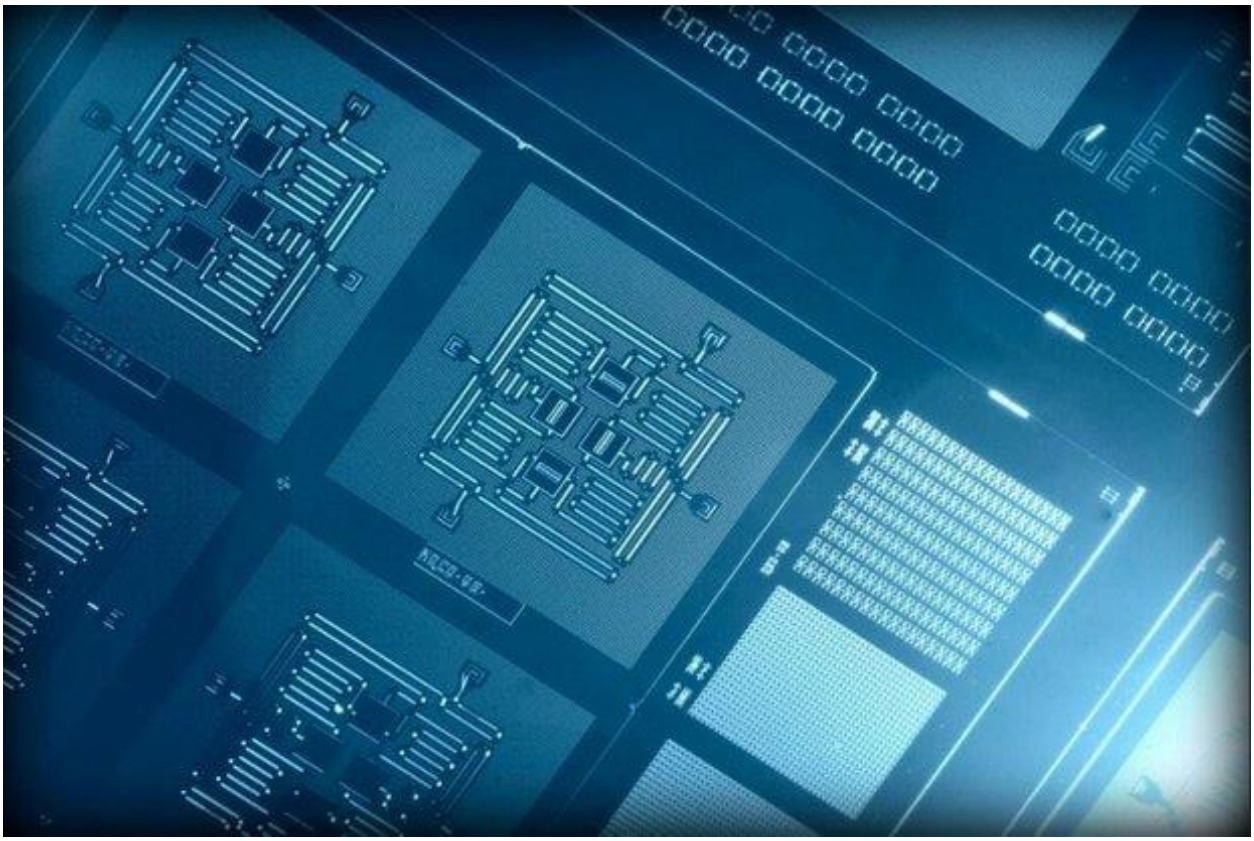
IBM Research is making its quantum processor available to the public via IBM's cloud to any desktop or mobile device.

"This moment represents the birth of quantum cloud computing," Arvind Krishna, senior vice president and director of IBM Research, said in a statement. "Quantum computers are very different from today's computers, not only in what they look like and are made of, but

more importantly in what they can do. Quantum computing is becoming a reality and it will extend computation far beyond what is imaginable with today's computers.

The cloud-enabled quantum computing platform, dubbed the IBM Quantum Experience, is designed to let researchers use individual quantum bits, also known as qubits, to run algorithms and experiments on IBM's quantum processor.

Jay Gambetta, manager of Theory of Quantum Computing and Information at IBM, told *Computerworld* that the public use of Quantum Experience will be free.



IBM's four qubit square circuit. (Photo by IBM)

"Since this is open to the public, there is no organization or business that will have priority," said Gambetta. "There are several opportunities for material and drug design, optimization, and other commercially important applications where quantum computing promises to offer significant value beyond what classical computers can offer."

Charles King, an analyst with Pund-IT, Inc., said IBM's 5-qubit processor should be powerful enough to handle a variety of research and other computations.

"I personally believe this is a very big deal," he added. "First and foremost, it should significantly broaden interest in and work around quantum computing. At this point, those efforts are mainly being performed by researchers associated with companies and labs able to afford highly experimental and highly expensive quantum technologies."

King also noted that providing public access should help validate work being done on quantum computing algorithms and applications, which previously could only be run in simulations.

"The project demonstrates that IBM's concepts around quantum processors work, can be reproduced and are stable enough to support cloud-based access and services," said King. "If the project succeeds and leads to a clearer understanding of quantum computing, as well as workable larger systems, it will definitely be remembered as a game changer."

Earl Joseph, an IDC analyst, noted that in addition to fully building a quantum computer, the big challenge is figuring out how to program it. IBM's move to engage the public should help with that.

"This experiment provides the opportunity for a large group of people to start to learn how to program quantum computers, which will help to develop ways to use this new type of technology," said Joseph. "Hopefully, it will help to motivate students to go into quantum computing programming as a field of research…. It's a milestone in allowing a larger number of people around the world to get their hands on this."

Richard Doherty, an analyst with The Envisioneering Group, called the IBM move a potential game changer.

"Quantum computers may be the most compelling, rich-data, cognitive engines for decades to come," he said. "Our eagerness to solve business, and societal IT and calculation challenges seems limitless. Data farms and smart data demand quantum computing power. If you make it, they will come. IBM and the public get to establish this."

Although D-Wave Systems Inc., a Canadian company, has said it's built a quantum computer and Google and NASA are testing their own quantum hardware, many in the computer industry and the world of physics say a full-scale quantum computer has not yet been created.

IBM isn't saying it's built a quantum computer. What it has are quantum processors, which are much smaller than a full-scale computer.

According to IBM, four to five qubits is the minimum number required to support quantum algorithms and simple applications. IBM's quantum processor contains five qubits.

The company noted that its scientists think in the next 10 years they'll have medium-sized quantum processors of 50 to 100 qubits, which they believe will be capable of tapping into quantum physics.

At 50 qubits, IBM contends that classic computers could not compete with it in terms of speed running complex calculations.

A quantum computer uses qubits, instead of the bits used in classic computers. A qubit has the possibility of being both a one and a zero. Using qubits, a quantum machine doesn't work in an orderly fashion and can calculate all possibilities at the same time.

That means quantum machines should be able to work on problems requiring complex and massive calculations much faster.

Scientists hope quantum computers will eventually be used to find distant habitable planets, create greater computer security and find a cure for cancer and heart disease.

IBM's quantum processor is being housed at the IBM T.J. Watson Research Center in New York.

"By giving hands-on access to IBM's experimental quantum systems, the IBM Quantum Experience will make it easier for researchers and the scientific community to accelerate innovations in the quantum field, and help discover new applications for this technology," Krishna said.