

# QUANTUM INFORMATION SCIENCE: DARPA'S NEW FRONTIER

By Craig Collins

It's been almost a half-century since Intel founder Gordon Moore first observed that ever-shrinking circuitry on silicon chips leads to the doubling of the performance of these chips every 18 months or so. This has been instrumental in bringing rapid progress to the field of information processing. The era of Moore's Law has been an interesting one, to say the least, but it is nearing its end: Within less than two decades, circuits will have shrunk to the atomic level.

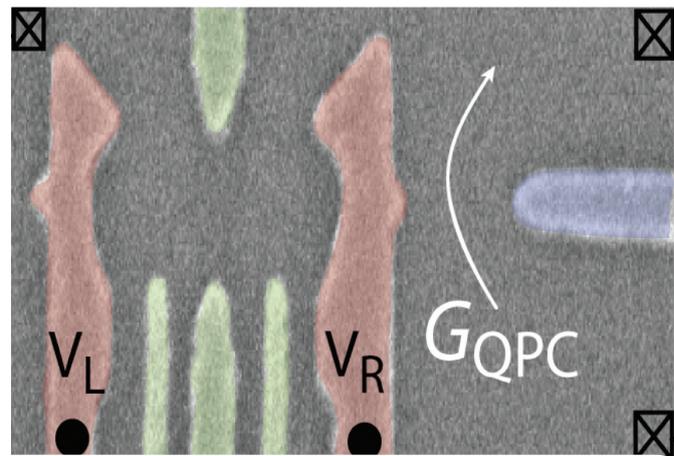
The problem – and more important, the challenge – with atom-sized circuits is that tiny objects don't behave the way matter and energy behave in our macroscopic world. They obey the strange and inscrutable laws of quantum mechanics. While atom-sized circuits may bring an end to Moore's Law, these quantum mechanical systems also bring new opportunities if their unique quantum properties can be harnessed.

It so happens that the manipulation of quantum systems has the potential to take speed, efficiency, and security to extremes unimaginable with classical information technology. The scientists who are today pioneering the field of quantum information science – a field that combines physics, information science, and mathematics – are creating a new physical paradigm of information theory that offers both quantitative and qualitative improvements in processing and transmission of information. In the process, they're learning completely new ways of describing and thinking about the physical world. And it should come as no surprise that the potential of quantum information technology is of significant interest to the U.S. defense and intelligence communities.

## QUANTUM INFORMATION

The first thing to understand about quantum information is that to most, it's incomprehensible. The only way the average person will ever know quantum information is through analogies and metaphors that vary in their precision. In the world we observe every day, the world of “classical mechanics” first described in elegant detail by Isaac Newton, it is comforting to know the apple always falls from the tree to the ground. In the bizarre microcosmos of the quantum realm, however, things are not so simple.

If it can be consistently controlled, however, the behavior of quantum systems offers clear advantages over today's digital information processing systems, which are based on “bits” – essentially, ones or zeroes – represented by the binary orientation of electrical switches, magnets, or lights. In quantum computing, ones and zeroes can be represented by the quantum properties of a molecule, set of molecules, or a photon – the smallest measurable quantity of light that

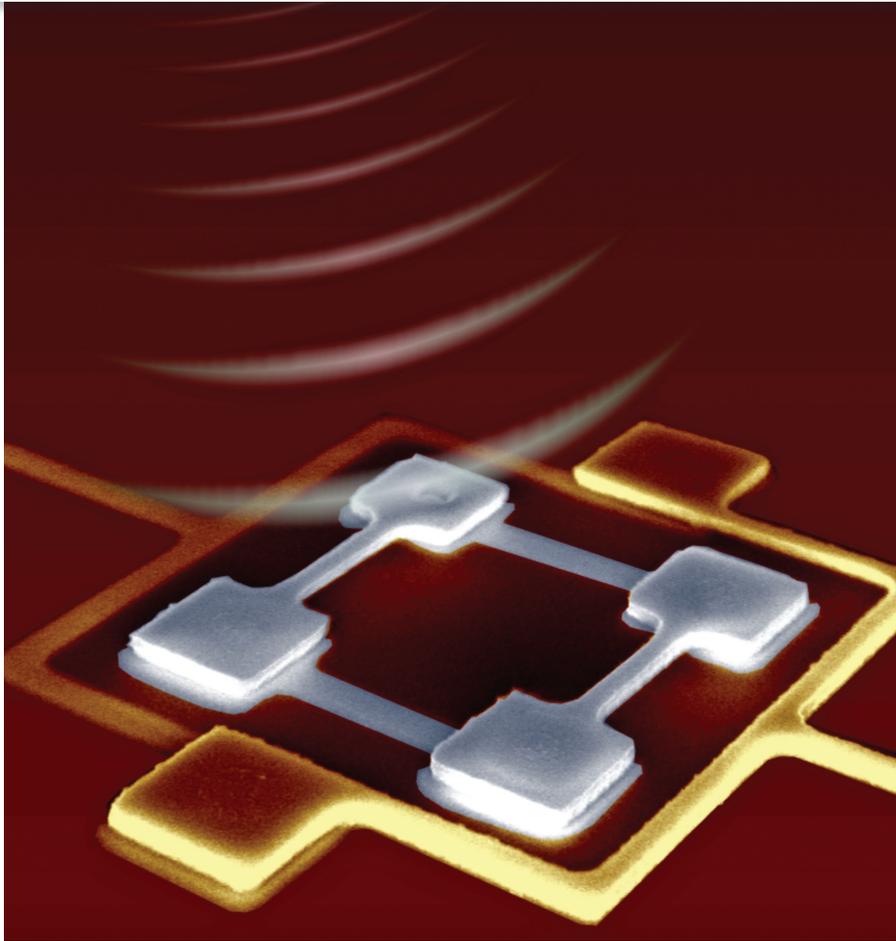


A double quantum dot device for semiconductor quantum computing: scanning electron micrograph showing electrostatic metal gates on the surface of a two-dimensional electron gas in gallium arsenide. Manipulation of voltages on the metallic gates (in red) allows formation of two single-electron spin qubits, which can be made to interact by changing the potential on the plunger gates (in green). Qubit states in the nearby quantum dot can be detected by quantum point contact (blue).

behaves, in certain ways, like an atomic particle. These quantum bits, or qubits, are superior to classical bits in two important ways: First, they can exist in a state of “superposition” in which they are literally in two distinguishable states at once – both one and zero – such as the internal electronic states of an atom, spin states of an atomic nucleus, or polarization states of a photon. Second, they can become “entangled” in a process that Albert Einstein called “spooky action at a distance” – quantum properties become synchronized when particles are placed close together, and retain this synchronization, like skilled dance partners, even after they're moved apart.

According to Dr. Jag Shah, a program manager with DARPA's Microsystems Technology Office, superposition and entanglement are

The superconducting flux quantum bit (blue loop) is cooled to 3 mK, a temperature close to absolute zero. Electric current traveling clockwise represents zero and current traveling counter-clockwise represents one. The qubit can also be in a superposition: current flowing both clockwise and counter-clockwise simultaneously (zero and one). The state of the qubit can be changed by applying the appropriate microwave field, and measured by a surrounding superconducting quantum interference device (SQUID, red).



what give quantum computing its tremendous power. “Two classical bits can represent zero, one, two, or three – but only one of those numbers,” he says. “Two quantum bits can represent ... all four numbers simultaneously. So that’s where the power of the quantum system comes in.” This exponential increase applies not only to storage, but also to information processing: These two qubits can execute not one, but four calculations in parallel. Exploiting this power of parallelism, a quantum computer could have far more power than a network of all the world’s supercomputers acting together.

DARPA, one of a handful of federal agencies to become increasingly excited about the field’s potential in the last decade, launched a five-year research program, the Quantum Information Science and Technology (QIST)

program, in 2001. Because it was investigating such a new and untested field, says Shah, the program was extremely broad in scope: “QIST addressed, for example, different types of physical systems, and the understanding of material science properties. Our researchers tried to advance the understanding of science – as well as tried to make more of these qubits and make them interact with each other.”

There is still much to investigate about quantum information processing, and the world’s first quantum computer is years, perhaps decades, from being realized. To date, the largest number of qubits ever contained within one quantum computing system is seven.

“One of the major problems of quantum systems,” says Shah, “is that this superposition state is a very fragile state. It only lasts for a short period of time, known as the dephas-

ing or decoherence time. And if that’s the case, how can you make the system work for a long period of time?” Right now, Shah says, researchers in quantum information science are still working at the building block level: “People are still worrying about how to create basic qubits that are robust [i.e., have long decoherence times], and [to understand] the material science involved, the physics involved: How do you develop control techniques for manipulating single and multiple qubits?”

#### QUANTUM COMMUNICATION: ALICE, BOB, AND EVE

The field of quantum communications – exploiting the quantum nature of photons – is somewhat further along than quantum processing. With the use of very weak laser pulses, single photons can be sent via air or fiber cable, detected with special receivers, and interpreted by customized equipment and software. The process, says Shah, is easier than quantum computing. “In some sense, it requires simpler quantum systems,” he says. “You’re talking about the transmission of single photons over a period of time. You’re not talking about putting together a large number of qubits in one place and controlling them and so on. The promise of quantum communications is secure communications; one of the issues with quantum communications is: How does it work in a real network?”

It’s still very difficult to build fast, reliable quantum channels, to process information gathered at high speeds, and to connect quantum links to networks that can transmit photons over significant distances. Today, single photons allow real-time data transmission only at very low speeds, a fraction of today’s fastest fiber-optic transmissions.

There is one application in quantum communications, however, that has advanced to the point where at least two private companies have developed a small-scale solution and introduced it to the marketplace: quantum key distribution, or QKD. In the QKD protocol, a quantum channel is used to build a shared

key, also called a one-time pad, between two parties, which can then be used to communicate over a classical channel securely. To understand how quantum key distribution works, consider three parties often used in cryptography parlance: Alice, Bob, and Eve. Alice sends a stream of photons to Bob, which maintain their quantum properties along the way (in other words, they aren't lost and don't decohere). Bob receives and measures the orientation of the photons, keeping track of what value he measures, and how he measured it. After repeating this process many times, Alice and Bob then communicate via a conventional channel about which photons were received and measured correctly. This leads to an encryption key known only to Alice and Bob. "It's a very elaborate process they have to go through," Shah says. "But it has been shown that if you can follow this procedure, and if it can be done in a way that approaches the accuracy that is needed, then any eavesdropper, Eve, is not able to detect the key that was transmitted from Alice to Bob." Like all inherently quantum objects, a photon in a superposition state collapses into a single orientation when observed – meaning that Eve cannot "read" a photon stream without altering it. Quantum encryption keys, then, are theoretically unbreakable. Thus, once the quantum communication generates a key shared by Alice and Bob alone, the two can communicate securely on regular channels at full speed.

In 2004, as part of the QuIST project, DARPA-funded researchers established the first QKD network to protect a fiber-optic loop connecting facilities at Harvard University, Boston University, and the office of BBN Technologies in Cambridge, Mass. "They determined important issues that need to be addressed," says Shah, "and they made a lot of progress. It's by no means a perfected system yet, but it is certainly [further] along than quantum processing is at this point."

Quantum key distribution does, however, have several significant limitations: Photons cannot travel far in air or over fiber-optic cables while maintaining their quantum information. The only way to achieve a system with total security in this kind of networking environment, at greater distances, is to add quantum repeaters – rudimentary quantum computers – to regenerate the qubits. Among the private companies currently developing

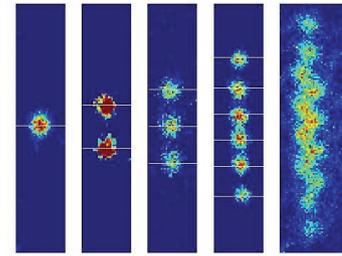
components needed to make quantum repeaters are NEC and Hewlett-Packard.

## THE QUANTUM FUTURE

A fully functioning quantum repeater is more likely to become operable before the world's first, full-fledged quantum processor, but researchers are enthusiastic about the potential of both to transform the way we think about processing and transmitting information. "Quantum key distribution is something that has excited people, because if it can really be made into a practical system, then it's a theoretically secure system of transmitting codes between two parties," says Shah.

Researchers in quantum information science, including Shah and other DARPA scientists, are equally excited about the possibility of someday using quantum computers to break encrypted codes – an application for which quantum processing presents an obvious solution. Enthusiasm surged in 1994 when a Bell Laboratories scientist named Peter Shor devised an algorithm for factoring large numbers on a quantum computer. As Shah points out: "Our public-key cryptology system is based on the factoring of large numbers" – figuring out which smaller prime numbers, when multiplied together, equal the larger number. "All of our commercial and military secure communications, everything is based on this. And as you make the code longer and longer, it takes more resources to do this factoring. If you use a classical processor, then the resources required to factor a large number increase exponentially with the size of the number. What Shor's algorithm showed was that by using quantum parallelism, the superposition states, and the ability to manipulate multiple numbers simultaneously, one can achieve a huge quantum speed-up."

While DARPA is understandably intrigued by the potential for quantum information science to transform encryption and cryptanalysis, there are other applications for which the power of quantum computing might prove useful: image processing, for example, or complex database searches, or the modeling of complex physical systems, which might be useful in the quest for new drugs or materials. "The question is," says Shah, "where else can this



False-color images of one, two, three, six, and 12 magnesium ions loaded into a planar ion trap. Red indicates areas of highest fluorescence, or the centers of the ions. As more ions are loaded in the trap, they squeeze closer together, until the 12-ion string falls into a zig-zag formation. Qubit states zero and one are encoded in stable internal states of the ion.

idea of quantum speed-up apply? There's a possibility that there will be other applications where quantum speed-ups can bring huge gains that will be not only of military interest, but also commercial interest." It's reasonable to believe that quantum information science, like all revolutionary scientific concepts, will have applications that nobody has yet conceived.

On the heels of its QuIST program, DARPA is still determining the best course for further investigation of quantum information science. Though no specific programs are yet in the works, says Shah, several are being discussed. "We want to try to determine the most challenging issues DARPA can address, and the best ways to address them. So that's the discussion we're having internally, and when we finish this process of discussion, we'll probably decide at that point whether we want to proceed with a program, and if so, what kind of a program."

One person who has no doubts about DARPA's future commitment to quantum information science is the agency's director, Dr. Anthony J. Tether. "Quantum information science is one of my 'future icons,'" says Tether. "I believe it will be known as a key DARPA accomplishment in the future. We continue to be interested in learning to exploit quantum phenomena, and I believe the technology holds the promise of opening new frontiers for the Department of Defense."