December 20, 2000

Eavesdroppers Beware: Single Photon Emission Prepares Way for Quantum Cryptography

Findings Also Enable Alternative Approach to Quantum Computation Using Photons as Qubits

Santa Barbara, Calif.--Researchers at the University of California at Santa Barbara (UCSB) report in the Dec. 22 issue of Science that they have built a device from which the emission of a single photon (particle of light) can be repeatedly detected. The ability to produce a single photon prepares the way for a whole new approach to communicating information secretly such that the information is unconditionally secure.

In addition to cryptography, the results also pertain more generally to the use of semiconductor quantum dots for quantum computation.

Quantum cryptography differs from other code schemes in that the attempt by a third party to intercept a code's key itself alters the key. It is as if the very act of listening in on a conversation makes the eavesdropper known.

Let us say that Alice wants to send a secret message to Bob. In order for the message to be secret, Alice has to employ some scheme to encode the message. And Bob needs a key to the scheme to decode the message. The crucial communication for the sake of preserving secrecy is not the message, but the key.

So Alice sends a string of single photons whose polarization successively contain the key. If a third party, Eve, tries to detect the singly transmitted photons, the act of detection causes an irreversible change in the wave function of the system. ("Wave function" denotes the quantum mechanical state of a physical system.) If Eve then tries to send the key on to Bob, the key will, in effect, bear the imprint of Eve's intermediate detection.

"Because measurements unavoidably modify the state of a single quantum system, an eavesdropper cannot gather information about the secret key without being noticed, provided that the pulses used in transmission do not contain two or more photons," state the researchers in the Science article.

Why is the single photon so important?

If the pulse that Alice sends contains two photons identically polarized (i.e., rotating the same way), Eve can in principle use a beam splitter to channel one of the photons into her detector while Bob receives the other photon. But if there is one and only one photon, it will have to choose in the presence of a beam splitter between Eve's and Bob's detectors. It is the singleness of the photon that guarantees security.

Though such a simplified example of quantum encryption may not seem convincingly foolproof, establishing a key with a single photon emission has been shown by Peter Shor of AT&T and John Preskill of Caltech to be secure from the most advanced attacks.

The eight UCSB researchers have built a device that produces that one photon emission upon which quantum

encryption depends. Three of the authors of the Science article, "A Quantum Dot Single-Photon Turnstile Device," are professors: Atac Imamoglu of Electrical and Computer Engineering (ECE) and of Physics, and Pierre Petroff and Evelyn Hu, both of ECE and Materials. The other authors have been either postdoctoral fellows (including first author Peter Michler) or graduate students associated with one of the faculty members' laboratories.

The device itself is mushroom-shaped and made out of semiconducting materials.

The first step was to grow a block of semiconducting materials layer by layer. Petroff's postdoc Winston Schoenfeld made the layered material using the technique molecular beam epitaxy or MBE. The base is a substrate of Gallium Arsenide. The post is made out of Aluminum Gallium Arsenide, and the ultra-thin mushroom cap or microdisk (200 nanometers thick) contains quantum dots of Indium Arsenide embedded in Gallium Arsenide.

A semiconductor quantum dot is a nanoscale box in which charge carriers are confined. These carriers can be electrons, holes (missing electrons), or excitons (bound electron-hole pairs). The carriers are confined because the band gap of the quantum dot material is lower than the band gap of the semiconducting material surrounding the quantum dot.

"Band gap" is the energy required to raise an electron from the valence band of the semiconductor crystal to its conduction band. With quantum dots, the higher band gap material of the surrounding material presents a potential barrier to the motion of the carriers out of the box. (Petroff developed the techniques to self-assemble quantum dots in 1993. He holds the patent.)

Hu and her graduate student Lidong Zhang took the block of layered material made by Petroff and Schoenfeld and shaped it into the device. "When we pattern and etch," said Hu, "we make use of the properties of the materials such that one etchant will work on one material and not another, and that ?s how we can form the po st without attacking the rest of the material."

The structure of the device--ultra-thin microdisk atop post--is so important because that shape enables the removal of most of the material surrounding the quantum dots. Less material surrounding the quantum dots means less material to contribute contaminating background radiation. The researchers did not knowingly choose the microdisk design in order deliberately to limit background radiation, but discovered that the disk design did so.

"People have made microdisks before," said Hu. "What's new here is combining that device with the quantum dot and with a knowledge of what to look for."

Imamoglu, his postdocs Michler and Christopher Becher, and his graduate student Alper Kiraz knew what to look for. They took the device, tailor-made by Petroff and Hu to make this measurement of a single photon emission, and actually made the measurements. Specifically, what they found when they used laser pulses to

load the quantum dots with energy is a pattern of subsequent emission without peaking. The lack of peaking indicates the singleness of photon emission.

"It's like God saying," quipped Petroff, "Let there be a photon, and there is a photon."

Imamoglu clarifies the nature of the measurement. It is not that only one photon is emitted from a quantum dot, but that among several photons emitted is one particular kind of photon. "The strong confinement enabled by the quantum dot structure ensures that the photons emitted are different, and we only look at the photon that is emitted at the lowest transition energy when the last electron-hole pair recombines."

One disadvantage of the microdisk for quantum cryptography is its lack of preferential output. But Imamoglu figures that some other shape, perhaps elliptical instead of circular, will cure that problem.

What really intrigues Imamoglu is the relevance of single photon emission to quantum computing. The idea behind quantum computing is to use particle spin as the quantum-bits or qubits analogous to the zero and one binary code of electronic computing.

Much of the theorizing about quantum computing has focused on the use of the spin states of electrons. But in a soon to be published paper, computer scientist Many Knill and physicist Raymond LaFlamme of Los Alamos National Laboratory and Gerald Milburn of Queensland University in Australia show that quantum computing can be done with linear optical elements. The one missing piece, say the authors, is the availability of a single photon emission source. And that, of course, is what the UC Santa Barbara researchers provide in this Science article.

Now, Imamoglu points out, instead of thinking about quantum computing strictly in terms of electron spin states as the qubits, there is an alternate approach which envisions the polarization of light as the qubits.

What is the advantage of using the nano structure in quantum dots as a means of generating photon qubits? "Speed and ease," said Imamoglu. "This all optical approach allows for a much faster way of doing real quantum operations. And photons are easy to deal with. We have a better chance of implementing a two-bit operation with this alternative scheme."

Note: Professor Imamoglu can be reached in Istanbul, Turkey, by phone at 011-90-216-308-3482 or by e-mail at atac@ece.ucsb.edu. Professor Petroff can be reached at (805) 893-8256. Professor Hu can be reached at 805-893-2368.

Images

Media Contact

Tony Rairden

trairden@engineering.ucsb.edu
805.893.4301