Long-Distance Quantum Message May Advance Code Making, Code Breaking

14 March 2007, for National Geographic News

An experiment on the Canary Islands, off the coast of Africa, has smashed a record for sending messages encrypted using the quirks of quantum physics.

The researchers transmitted particles of light, or photons, 90 miles (144 kilometers) while keeping intact a strange invisible tie between the particles known as entanglement.

The demonstration shows that it would be possible to build a network of satellites that could beam ultra-secure messages between themselves and to Earth, researchers say.

Because of the unique and complex properties of entanglement, there is virtually no chance such messages could ever be successfully intercepted and decoded.

And the techniques used in the experiment could also be useful in creating quantum computers, which could exploit quantum physics to solve in seconds problems that would take today's machines years of work.

Quantum Message

In the experiment, a light beam carried a message from the island of La Palma to Tenerife, where a receiver was able to spot individual photons (see of map of the Canary Islands).

The transmission was ten times farther than anyone has been able to send entangled photons through the air before.

It's even farther than previous records for sending these signals through fiber-optic cables, like those used as telephone wires. (Related: "Physicists Teleport Quantum Bits Over Long Distance" [January 29, 2003].)

The work was published in the journal *Physical Review Letters* in January and presented at a meeting of the American Physical Society last week.

Unbreakable Code

When two particles become entangled, manipulating one instantly affects the other, no matter how far apart they are.

No one knows exactly how particles remain entangled. Albert Einstein even once called the phenomenon "spooky action at a distance."

Anton Zeilinger, leader of the new study, likened the entanglement to a set of trick dice, which he calls quantum dice.

"Quantum dice have the funny feature that if you open the pack and throw them, they show the same number, independent of how far they are separated from each other," Zeilinger said.

"You cannot buy these yet, but I'm sure in a hundred years they will be under the Christmas tree," he joked.

That's because his and others' experiments are revealing increasing control over individual atoms, electrons, and photons—including methods to create and manipulate entangled pairs.

For example, when researchers made a measurement of an entangled photon that remained at La Palma, it instantly affected the particle's counterpart—regardless of whether it was in mid-flight or had already arrived at Tenerife.

In this way, entanglement can be used to send ultra-secure messages to people far away.

If anyone tried to eavesdrop on such a message, it would disrupt the entanglement, alerting the receiver that security has been compromised.

The receiver would tell the sender not to beam over the key used to decode the message. Instead the pair would start over with a new message encrypted with a new key.

The research "is a real technological tour de force," said Nicolas Gisin of the University of Geneva in Switzerland, who has also worked on long-distance entanglement.

Satellite Network

The new experiment shows it is possible to send entangled photons over long distances through the air, so it should be possible to send them to satellites or the International Space Station, study leader Zeilinger added.

Those satellites would be able to send quantum-encrypted messages between each other or back to any location on Earth, he said.

Showing that this is possible "is in my opinion the major value of this experiment," Gisin, of the University of Geneva, added.

There are some major obstacles to using the method commercially, however, he pointed out. The rate of information sent was low, and the transmission only worked at night when the weather cooperated.

Beyond making communications more secure, entanglement has other important uses.

Entanglement is crucial in creating quantum computers, a powerful type of computer that works in a fundamentally different way than current technology.

One of the most promising applications for quantum computers is the ability to rapidly factor large numbers, a task that is very difficult for modern machines.

Current encryption practices, such as those used for online shopping sites, take advantage of this difficulty. By multiplying huge numbers together, codes are created that would take years or decades of computing time to factor.

Because quantum computers work in a completely different fashion, however, a large one could factor enormously long numbers very quickly—rendering today's methods of encryption obsolete.

Researchers have already built very basic devices—made of entangled photons whizzing around or atoms trapped in place by lasers—that can do simple calculations, such as factoring the number 21 to show it is equal to 3 times 7.

But quantum computers powerful enough to crack huge numbers are a long way off, probably decades.

Even if they do come to fruition, however, they may not be used for these kinds of calculations.

"I personally feel quantum computers will not be for factorization of large numbers," Zeilinger said. "As soon as you know you can do it, no one will use factorization for encoding secret messages."