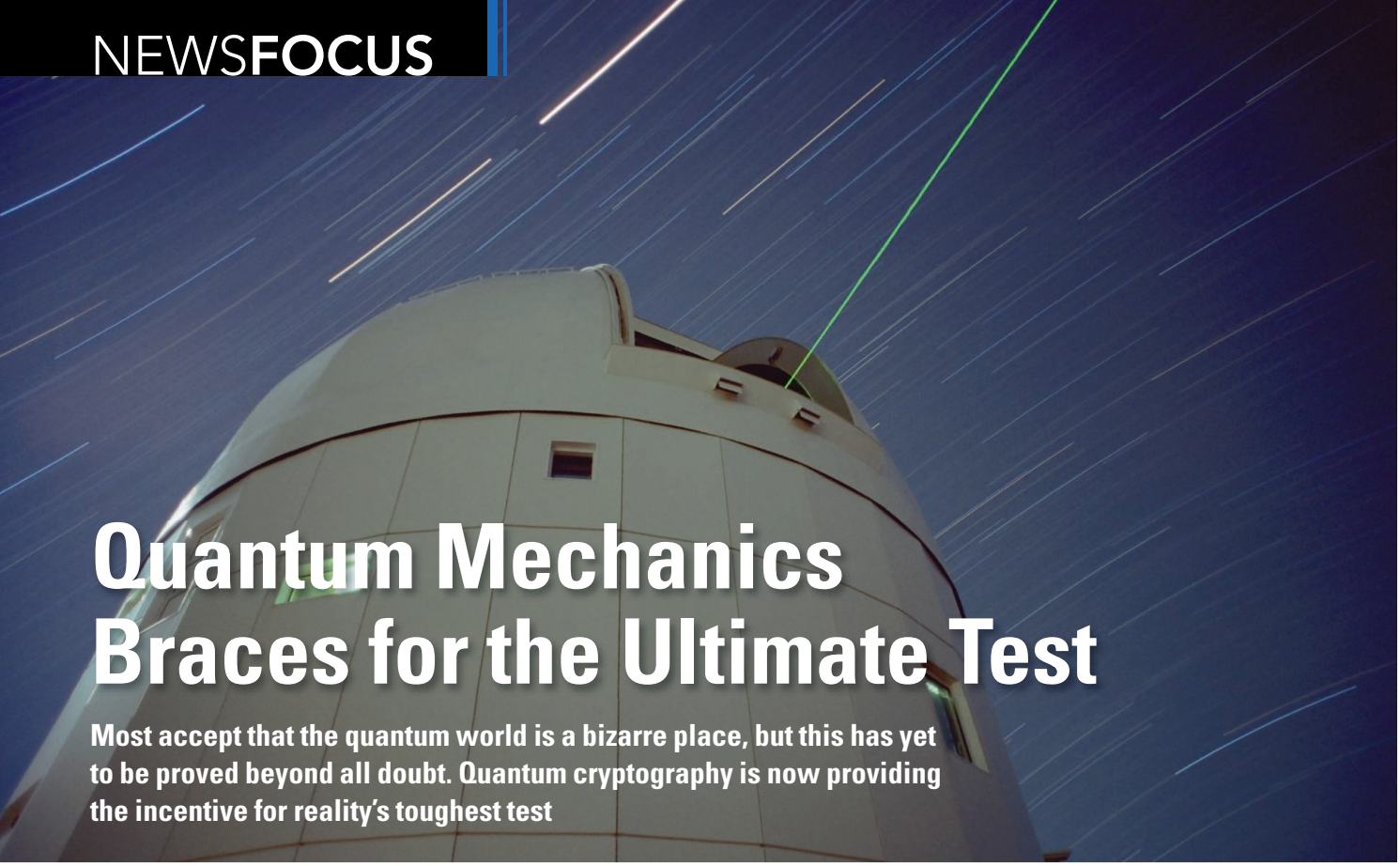


Quantum Mechanics Braces for the Ultimate Test

Most accept that the quantum world is a bizarre place, but this has yet to be proved beyond all doubt. Quantum cryptography is now providing the incentive for reality's toughest test

THE 2010 SOCCER WORLD CUP IN SOUTH Africa marked a milestone for Nicolas Gisin, although he is not a sportsman and his national team, Switzerland, did not win. A physicist by trade, Gisin views the championship with pride because it was the first international public event to employ an ultratight security system, devised by his Geneva-based company ID Quantique, that harnesses the weird workings of quantum physics to protect sensitive information. Now Gisin, of the University of Geneva, is on a quest to build the ultimate quantum cryptography system: one that users could trust implicitly, even if they had bought it from their worst enemy. First, however, Gisin and others have to plug a few stubborn holes in one of the bedrocks of modern physics.

Quantum mechanics is one of physics' most resounding successes, accurately describing everything from the internal workings of the atom to the structure of DNA and the makeup of neutron stars. It's spawned a wealth of technology, too, including electronics, computers, lasers, fiber optics, and nuclear power. But there's a fly in the ointment: The microscopic world that quantum mechanics describes is a bizarre place where nothing is certain and the act of observation changes things. Some physicists over the past century, including Einstein, have refused to accept that this is the only possible description of reality. Over the past 40 years, that description has been put to the test in a series of elegant experiments that have shown it to be true. Although most physicists find the results convincing, these experiments did skirt around a few tiny loopholes by which reality could have fooled physicists into thinking that quantum mechanics paints a complete picture.

It's these loopholes that Gisin's team and a number of other groups around the world are competing to close. The winners will have the satisfaction of settling one of the most stubborn problems in physics. As a bonus, they will also hold the key to the perfect quantum security system. "This race is on because the group that performs the first loophole-free test will have an experiment that stands in history," Gisin says.

Curiouser and curiouser

Despite its near-ubiquity in physics, quantum mechanics retains its ability to make heads spin, says Antonio Acín, a collaborator of Gisin's at the Institute of Photonic Sciences in Barcelona, Spain. Two of its most mind-scrambling features lie at the heart of quantum cryptography. The first, known as superposition, tells you that before you look, an object such as an electron can exist in two different places at the same time, or simultaneously hold two mutually exclusive properties—such as having a high or a low energy state. Only when someone measures it are the electron's multiple personalities forced to snap into one identity, with a single location and a definite energy state. Before measurement, there's no way to predict with certainty which identity it will choose; the outcome is always random.

The second property, known as nonlocality, is even stranger. It says that if, for example, two particles can be entangled—twinned together in the lab in such a way that when measured their properties correlate—then they will remain entangled even if vast distances separate them at the time of measurement. Because superposition dictates that properties don't take a fixed value until measured, one particle of the pair must somehow "know" the result of its twin's measurement. "It's as shocking as taking two dice to opposite ends of the universe and rolling them simultaneously, only to find that each time they always land on the same number," Acín says.

Toward the end of the 20th century, physicists realized that these mind-boggling properties could be harnessed to shore up the transmission of sensitive messages across the Internet. Standard cryptographic techniques work by scrambling transmissions with a secret "key"—a string of zeros and ones—that the sender and the receiver share. The key is generated by a computer algorithm, but if that is cracked, an eavesdropper can read the message.

Throwing in entanglement makes the

CREDIT: ©LOQO/I-WIEN

Published by AAAS

Long shot. Researchers beam a succession of entangled photons from a telescope in La Palma 144 kilometers to the neighboring island of Tenerife to test quantum mechanics.

eavesdropper's task much tougher, however. Suppose you entangle several pairs of particles and give both the sender and the receiver one member of each pair. Just before transmitting a message, the sender can measure the energy levels of his or her particles and assign either a zero or a one depending on the value. The resulting string of ones and zeroes can serve as a cryptographic key. By performing similar measurements on the particles' counterparts, the receiver will get an identical key, even from halfway across the universe. Because the outcome of quantum measurements can't be predicted, the key will be truly random. What's more, because quantum superpositions are disrupted whenever you look at them, any eavesdroppers trying to read the key beforehand will leave telltale evidence of their presence.

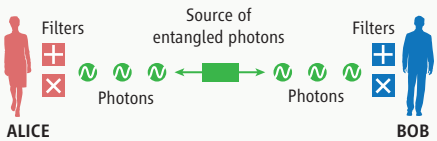
Gisin's ID Quantique is one of a handful of companies that already employ such quantum tricks in commercial applications. But Gisin and Acín want to beef up security further, producing a system so trustworthy users could buy it as a black box from a hacker and still be confident that the key it generated was secure thanks to its quantum origins. "Without that assurance, you cannot be certain that your black box isn't just spewing out a copy of a string of zeros and ones, preprogrammed by the hacker," Acín says.

Their work is based on the idea of device-independent quantum cryptography put forward in 1991 by physicist Artur Ekert, now at the Centre for Quantum Technologies in Singapore. Ekert realized that, in principle, the same tests that physicists used to prove nonlocality in the lab could be incorporated into a cryptographic system. In 2009, Gisin, Acín, and colleagues proposed a practical setup for "a box that certifies its quantum credentials at the push of a button, each time it produces a key," Acín says. Last year, Acín and colleagues took a tantalizing step toward making such a box by demonstrating that the tests could be integrated into a machine that generates random numbers using entanglement.

But the new security protocol is only as tight as the tests historically used to prove nonlocality—and that's where things get a little hairy. "Those were fantastic, beautiful experiments, but they had some shortcomings," explains Anton Zeilinger, an expert on entanglement at the University of Vienna. The tests were originally inspired by a theoretical challenge that Einstein threw down against quantum mechanics—but it's a challenge that, technically, has not yet quite been met.

EKERT'S QUANTUM CRYPTOGRAPHY

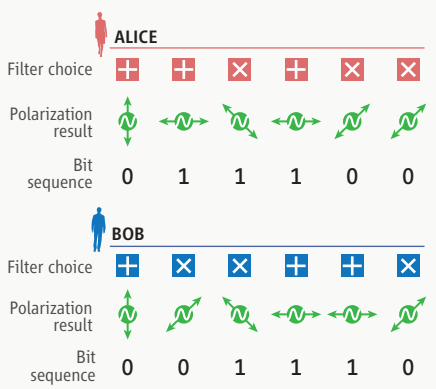
Step 1: One photon from each entangled pair is sent to Alice and the other is sent to Bob.



Step 2: Alice and Bob choose one of two filters at random to measure the direction of polarization of each photon that they receive.

Filter choice	Possible results
+	↕ ↔
×	⤢ ⤡
Bit value assigned	0 1

Step 3: From the polarization results, Alice and Bob each generate a sequence of bit values.



Step 4: Alice and Bob openly confer about which filters they used for each photon (but not the results). Their shared secret key is made up of the bit values generated when their filter choices matched.

Step 5: If an eavesdropper attempts to intercept any photons, the quantum correlations between the pairs are destroyed. Alice and Bob can check for this by performing a Bell test using a third filter on the photon pairs. If their correlations do not violate Bell's bound, then the system has been hacked.

SOURCE: ZEEVA MERALI

Einstein's bugbear

Nonlocality famously galled Einstein, who derided the idea that two particles could inexplicably and instantaneously coordinate their properties as "spooky action at a distance." In 1935, along with Boris Podolsky and Nathan Rosen, Einstein described a thought experiment that sought to show that nonlocality was absurd and quantum mechanics could never provide the final word on how the world works. Instead, he argued, the behavior of entangled particles could be explained far less mysteriously if they were preprogrammed by a set of unseen blueprints—or "hidden variables."

Einstein's position is known as local realism: Particles can't communicate instantaneously over vast distances, and their properties are real and there all the time, irrespective of measurement. Thirty years after Einstein, Podolsky, and Rosen posed their thought experiment, another physicist tried to turn it into a real one. In 1964, John Bell, a British physicist working at the CERN particle physics lab near Geneva, defined the maximum level of correlations between two entangled particles that hidden variables could explain. If a correlation exceeded Bell's limits, then local realism was violated and reality was far spookier than nonquantum physics allowed. "When I read John Bell's paper, it was like love at first sight," says Alain Aspect of the Institute of Optics in Palaiseau, France.

In the 1980s, Aspect and his colleagues set up an experiment in which pairs of photons—single particles of light—were entangled in such a way that no matter which direction they chose to measure their polarization (which could be either "parallel" or "perpendicular" to the direction of measurement), they always tallied.

Just as a police officer interrogating two suspects must keep them separated so that they do not confer, Aspect had to close any "communication loopholes" in the test. This meant ensuring that the two photons were far enough apart and that his measurements were performed fast enough that the pair could not influence each other without exchanging information faster than the speed of light, the universe's speed limit. Aspect did this by using a fast generator that changed the direction in which to measure the photons' polarizations while the photons were flying away from each other, so that they were too distant to communicate their results when the choice was made. Even with this restriction in place, Aspect found that the polarizations of the particles matched up to a degree that violated Bell's inequalities and so contradicted local realism.

The now-celebrated Aspect experiment, along with similar ones, helped to write nonlocality into physics textbooks. But there is another loophole that those experiments did

Published by AAAS

not close. The trouble is that photons are slippery customers: small, fast, and notoriously hard to detect. Typically, if five photons are hurled at a detector, it will register only one. That means that physicists can trust that Bell's bound has been violated only if they assume that the photons caught provide a fair representation of how all the photons in the experiment behaved—much the way exit polls at voting booths predict election results.

Most physicists accept that the fair-sampling assumption is a good one. "It's unlikely that nature is so malicious that it conspires with the apparatus to hold back particular photons just to fool us into thinking that quantum mechanics works," Gisin says.

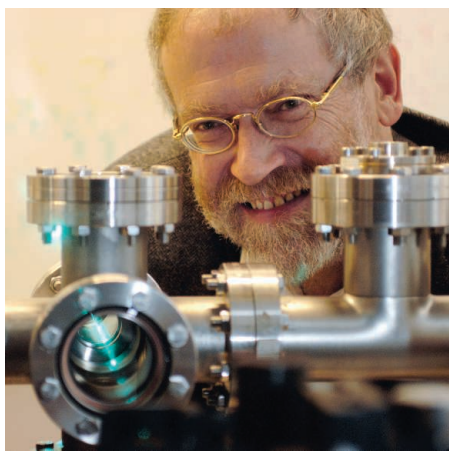
Nonetheless, physicists hate loose ends, so the chase to find a perfect, loophole-free test has continued over the past decade. "Until the test is done, we can't honestly say that hidden variables have been ruled out—even if the consensus is they don't make sense—because we haven't proved it," says Harald Weinfurter of the Ludwig Maximilian University in Munich, Germany.

The detection loophole is also bad news for cryptographers. While it remains open, a Bell test cannot certify that a black box is working according to quantum rules. "A hacker—by definition—is malicious enough to exploit the detection loophole to fool us into thinking that a quantum process has taken place," Gisin says. As a result, Acín adds, "suddenly, this most philosophical of experiments, the loophole-free Bell test, has a practical purpose, with commercial rewards." The first group to perform it will immediately be in place to make a device-independent quantum cryptographic system.

Closing the loops

With their eyes on the prize, a group led by Paul Kwiat of the University of Illinois, Urbana-Champaign, has been collaborating with engineers at the U.S. National Institute of Standards and Technology (NIST) in Boulder, Colorado, to develop photon detectors with near 100% efficiency. "Those are good enough to perform a loophole-free test," says team member Joseph Altepeter of Northwestern University in Evanston, Illinois. The struggle now is to chain these components together with optical fibers across a large enough distance to keep the communication loophole shut. "Essentially the pieces are all in place, but the devil is in the detail," Altepeter says.

Meanwhile, Weinfurter and his colleagues are tackling the problem from an entirely different angle. They were inspired by an experiment, carried out in 2001 by David Wineland's team at NIST, that successfully closed the detection loophole using atoms rather than photons. Because atoms are far more hefty than flighty photons, Wineland realized, they are less likely to escape the apparatus, so they provide a potentially perfect detection rate. The team performed a Bell test that compared how often the energy levels—high or low—of electrons in entangled pairs of atoms matched up. Once again, quantum mechanics was hailed victorious, as the level of correlations exceeded Bell's inequalities. But



Earlier quantum tests "had some shortcomings."

—ANTON ZEILINGER, UNIVERSITY OF VIENNA

it was not a resounding win because the atoms were close enough together to have influenced each other. In other words, the researchers had closed the detection loophole but in the process were forced to leave the communication loophole open.

Building on Wineland's experiment, Weinfurter's group is attempting to tie up both loopholes at once, by weaving photons together with atoms to reap the benefits of both. The idea is to start with two initially unentangled atoms in separate laboratories—ideally more than 100 meters apart, so that the atoms cannot influence each other over the course of the test. Each atom emits a photon; the two photons are captured and transmitted along optical fibers to a third location, where they are entangled. "The magic is that as soon as the photons are entangled, their parent atoms automatically become entangled, too," explains Weinfurter's collaborator Marek Zukowski at the University of Gdansk in Poland.

These newly entangled atoms can then take the Bell test, with a perfect detection rate, while sitting far enough apart to keep the communication loophole closed. "The setup is being tried in two neighboring labs right now," Zukowski says. "When we are happy that everything is working, we will try it in two distant labs."

If Weinfurter can simultaneously close the detection and communication loopholes, then the verification of Bell's tests of quantum mechanics will be complete. Or will it? In the most mind-bending possible loophole of all, Bell and others have raised the possibility that experimenters may not have the free will to carry out the experiments anyway. Hidden variables, Zeilinger explains, might also be either shackling the hands of experimenters or controlling their apparatus to somehow manipulate the choice of which photon properties are measured. This could distort the results, making it appear that quantum mechanics is valid when it is not.

In a virtuoso display of long-distance entanglement, Zeilinger and colleagues ruled out this possibility. They generated entangled photon pairs at an observatory in La Palma in the Canary Islands and then fired one of them through the night sky to the neighboring island of Tenerife, where it was caught in a telescope belonging to the European Space Agency. They used random number generators to decide which measurements to make on the photons while they were in flight. But crucially, they placed a random number generator at a third, distant location on La Palma to ensure that its output could not have been influenced by hidden variables produced alongside the photons.

"We confirmed that Bell's limit was violated, while closing both the communication and, for the first time, the freedom-of-choice loopholes," Zeilinger says. Gisin commends the group for closing this little-known loophole. But he adds that it remains possible that hidden variables produced before the experiment began—perhaps even reaching as far back as the big bang—are predetermining all our actions. "It will be impossible to test against that type of superdeterminism," he says.

With quantum cryptography injecting momentum, Zukowski thinks the race to close all the loopholes simultaneously will soon be over. "Conservatively, it could take another 5 years to complete, but it could also be done tomorrow," he says. "We're at the stage where everyone is scared to read their competitors' papers, in case they find they have been beaten. The only real question is: Who will win?"

–ZEEYA MERALI

Zeeya Merali is a freelance writer based in London.

Published by AAAS