Three groups close the loopholes in tests of Bell's theorem

Until now, the quintessential demonstration of quantum entanglement has required extra assumptions.

FRANK AUPERLE

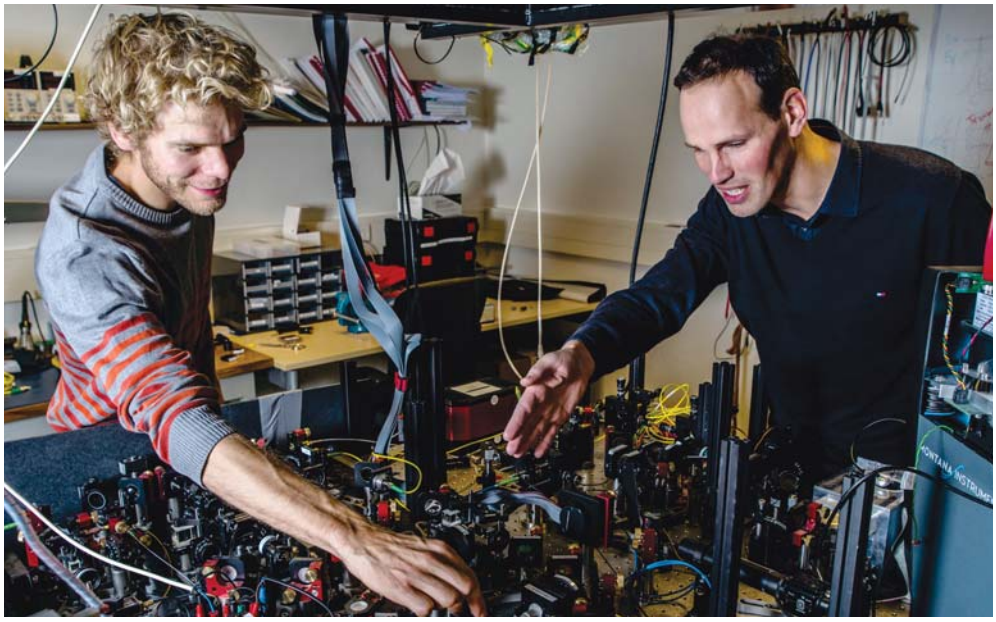

FIGURE 1. BAS HENSEN (LEFT) AND RONALD HANSON in one of the three labs they used for their Bell test.

The predictions of quantum mechanics are often difficult to reconcile with intuitions about the classical world. Whereas classical particles have well-defined positions and momenta, quantum wavefunctions give only the probability distributions of those quantities. What's more, quantum theory posits that when two systems are entangled, a measurement on one instantly changes the wavefunction of the other, no matter how distant.

Might those counterintuitive effects be illusory? Perhaps quantum theory could be supplemented by a system of hidden variables that restore local realism, so every measurement's outcome depends only on events in its past light cone. In a 1964 theorem John Bell showed that the question is not merely philosophical: By looking at the correlations in a series of measurements on widely separated systems, one can distinguish quantum mechanics from any local-realist theory. (See the article by Reinhold Bertlmann, PHYSICS TODAY, July 2015, page 40.) Such Bell tests in the laboratory have come down on the side of quantum mechanics. But until recently, their experimental limitations have left open two important loopholes that require additional assumptions to definitively rule out local realism.

Now three groups have reported experiments that close both loopholes simultaneously. First, Ronald Hanson, Bas Hensen (both pictured in figure 1), and their colleagues at Delft University of Technology performed a loophole-free Bell test using a novel entanglement-swapping scheme.[1] More recently, two groups—one led by Sae Woo Nam and Krister Shalm of NIST,[2] the other by Anton Zeilinger and Marissa Giustina of the University of Vienna[3]—used a more conventional setup with pairs of entangled photons generated at a central source.

The results fulfill a long-standing goal, not so much to squelch any remaining doubts that quantum mechanics is real and complete, but to develop new capabilities in quantum information and security. A loophole-free Bell test demonstrates not only that particles can be entangled at all but also that a particular source of entangled particles is working as intended and hasn't been tampered with. Applications include perfectly secure quantum key distribution and unhackable sources of truly random numbers.

Locality and detection

In a typical Bell test trial, Alice and Bob each possess one of a pair of entangled particles, such as polarization-entangled photons or spin-entangled electrons. Each of them makes a random and independent choice of a basis—a direction in which to measure the particle's polarization or spin—and performs the corresponding measurement. Under quantum mechanics, the results of Alice's and Bob's measurements over repeated trials can be highly correlated—even though their individual outcomes can't be foreknown. In contrast, local-realist theories posit that only local variables, such as the state of the particle, can influence the outcome of a measurement. Under any such theory, the correlation between Alice's and Bob's measurements is much less.

But what if some hidden signal informs Bob's experiment about Alice's choice of basis, or vice versa? If such a signal can change the state of Bob's particle, it can create quantum-like correlations in a system without actual quantum entanglement. That possibility is at the heart of the so-called locality loophole. The loophole can be closed by arranging the experiment, as shown in figure 2, so that no light-speed signal with information about Alice's choice of basis can reach Bob until after his measurement is complete.

In practice, under that arrangement, for Alice and Bob to have enough time to choose their bases and make their measurements, they must be positioned at least tens of meters apart. That requirement typically means that the experiments are done with entangled photons, which can be transported over such distances without much damage to their quantum state. But the inefficiencies in handling and detecting single photons introduce another loophole, called the fair-sampling or detection loophole: If too many trials go undetected by Alice, Bob, or both, it's

possible for the detected trials to display quantum-like correlations even when the set of all trials does not.

In Bell tests that are implemented honestly, there's little reason to think that the detected trials are anything other than a representative sample of all trials. But one can exploit the detection loophole to fool the test on purpose by causing trials to go undetected for reasons other than random chance. For example, manifestly classical states of light can mimic single photons in one basis but go entirely undetected in another (see PHYSICS TODAY, December 2011, page 20). Furthermore, similar tricks can be used for hacking quantum cryptography systems. The only way to guarantee that a hacker is not present is to close the loopholes.

Solid-state spins

Instead of the usual entangled photons, the Delft group based their experiment on entangled diamond nitrogen–vacancy (NV) centers, electron spins associated with point defects in the diamond's crystal lattice and prized for their long quantum coherence times. The scheme is sketched in figure 3: Each NV center is first entangled with a photon, then the photons are sent to a central location and jointly measured. A successful joint measurement, which transfers the entanglement to the two NV centers, signals Alice and Bob that the Bell test trial is ready to proceed.

In 2013 the team carried out a version of that experiment[4] with the NV spins separated by 3 m. "It was at that moment," says Hanson, "that I realized that we could do a loophole-free Bell test—and also that we could be the first." A 3-m separation is not enough to close the locality loophole, so the researchers set about relocating the NV-center equipment to two separate labs 1.3 km apart and fiber-optically linking them to the joint-measurement apparatus at a third lab in between.

A crucial aspect of the entanglement-swapping scheme is that the Bell test trial doesn't begin until the joint measurement is made. As far as the detection loophole is concerned, attempted trials without a successful joint measurement don't count. That's fortunate, because the joint measurement succeeds in just one out of every 156 million attempts—a little more than once per hour.

That inefficiency stems from two main sources. First, the initial spin–photon entanglement succeeds just 3% of the time at each end. Second, photon loss in the optical fibers is substantial: The photons entangled with the NV centers have a wavelength of 637 nm, well outside the so-called telecom band, 1520–1610 nm, where optical fibers work best. In contrast, once the NV spins are entangled, they can be measured efficiently and accurately. So of the Bell test trials that the researchers are able to perform, none are lost to nondetection.

Early in the summer of 2015, Hanson and colleagues ran their experiment for 220 hours over 18 days and obtained 245 useful trials. They saw clear evidence of quantum correlations—although with so few trials, the likelihood of a nonquantum system producing the same correlations by chance is as much as 4%.

The Delft researchers are working on improving their system by converting their photons into the telecom band. Hanson estimates that they could then extend the separation between the NV centers from 1.3 km up to 100 km. That distance makes feasible a number of quantum network applications, such as quantum key distribution.

In quantum key distribution—as in a Bell test—Alice and Bob perform independently chosen measurements on a series of entangled particles. On trials for which Alice and Bob have fortuitously chosen to measure their particles in the same basis, their results are perfectly correlated. By conferring publicly to determine which trials those were, then looking privately at their measurement results for those trials, they can obtain a secret string of ones and zeros that only they know. (See article by Daniel Gottesman and Hoi-Kwong Lo, PHYSICS TODAY, November 2000, page 22.)

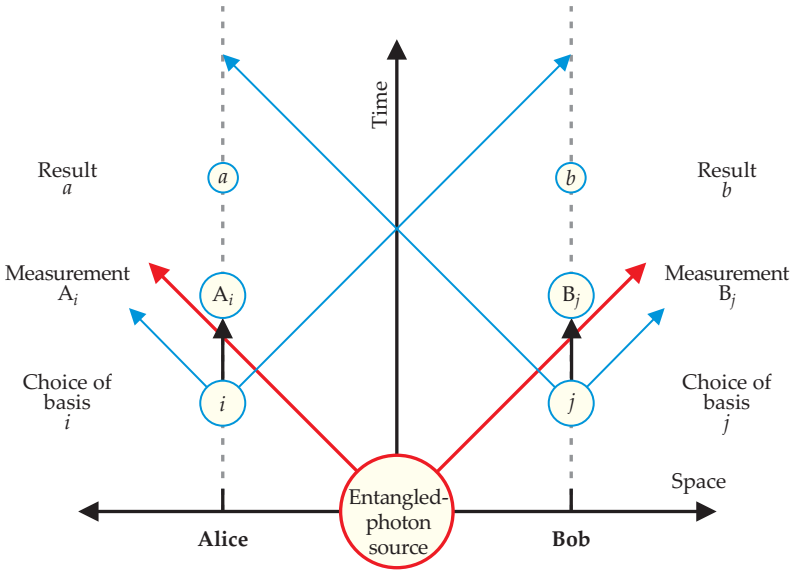

FIGURE 2. THE LOCALITY LOOPHOLE arises from the possibility that hidden signals between Alice and Bob can influence the results of their measurements. This space–time diagram represents an entangled-photon experiment for which the loophole is closed. The diagonal lines denote light-speed trajectories: The paths of the entangled photons are shown in red, and the forward light cones of the measurement-basis choices are shown in blue. Note that Bob cannot receive information about Alice's chosen basis until after his measurement is complete, and vice versa.

Efficient detectors

The NIST and Vienna groups both performed their experiments with photons, and both used single-photon detectors developed by Nam and his NIST colleagues. The Vienna group used so-called transition-edge sensors that are more than 98% efficient;[5] the NIST group used superconducting nanowire single-photon detectors (SNSPDs), which are not as efficient but have far better timing resolution. Previous SNSPDs had been limited to 70% efficiency at telecom wavelengths—in part because the polycrystalline superconductor of choice doesn't couple well to other optical elements. By switching to an amorphous superconducting material, Nam and company increased the detection efficiency to more than 90%.[6]

Shalm realized that the new SNSPDs might be good enough for a loophole-free

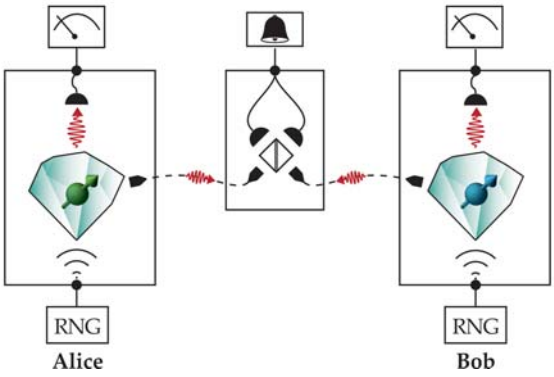

FIGURE 3. ENTANGLEMENT SWAPPING between diamond nitrogen–vacancy (NV) centers. Alice and Bob entangle their NV spins with photons, then transmit the photons to a central location to be jointly measured. After a successful joint measurement, which signals that the NV spins are entangled with each other, each spin is measured in a basis chosen by a random-number generator (RNG). (Adapted from ref. 1.)

Bell test. "We had the detectors that worked at telecom wavelengths, so we had to generate entangled photons at the same wavelengths," he says. "That was a big engineering challenge." Another challenge was to boost the efficiency of the mazes of optics that carry the entangled photons from the source to the detector. "Normally, every time photons enter or exit an optical fiber, the coupling is only about 80% efficient," explains Shalm. "We needed to get that up to 95%. We were worrying about every quarter of a percent."

In September 2015 the NIST group conducted its experiment between two laboratory rooms separated by 185 m. The Vienna researchers positioned their detectors 60 m apart in the subbasement of the Vienna Hofburg Castle. Both groups had refined their overall system efficiencies so that each detector registered 75% or more of the photons created by the source—enough to close the detection loophole.

In contrast to the Delft group's rate of one trial per hour, the NIST and Vienna groups were able to conduct thousands of trials per second; they each collected enough data in less than one hour to eliminate any possibility that their correlations could have arisen from random chance.

It's not currently feasible to extend the entangled-photon experiments into large-scale quantum networks. Even at telecom wavelengths, photons traversing the optical fibers are lost at a nonnegligible rate, so lengthening the fibers would lower the fraction of detected trials and reopen the detection loophole. The NIST group is working on using its experiment for quantum random-number generation, which doesn't require the photons to be conveyed over such vast distances.

Random numbers are widely used in security applications. For example, one common system of public-key cryptography involves choosing at random two large prime numbers, keeping them private, but making their product public. Messages can be encrypted by anyone who knows the product, but they can be decrypted only by someone who knows the two prime factors.

The scheme is secure because factorizing a large number is a computationally hard problem. But it loses that security if the process used to choose the prime numbers can be predicted or reproduced. Numbers chosen by computer are at best pseudorandom because computers can run only deterministic algorithms. But numbers derived from the measurement of quantum states—whose quantum nature is verified through a loophole-free Bell test—can be truly random and unpredictable.

The NIST researchers plan to make their random-number stream publicly available to everyone, so it can't be used for encryption keys that need to be kept private. But a verified public source of tamperproof random numbers has other uses, such as choosing unpredictable samples of voters for opinion polling, taxpayers for audits, or products for safety testing.

Johanna Miller

References

1. B. Hensen et al., *Nature* **526**, 682 (2015).
2. L. K. Shalm et al., *Phys. Rev. Lett.* (in press), http://arxiv.org/abs/1511.03189.
3. M. Giustina et al., *Phys. Rev. Lett.* (in press), http://arxiv.org/abs/1511.03190.
4. H. Bernien et al., *Nature* **497**, 86 (2013).
5. A. E. Lita, A. J. Miller, S. W. Nam, *Opt. Express* **16**, 3032 (2008).
6. F. Marsili et al., *Nat. Photonics* **7**, 210 (2013).