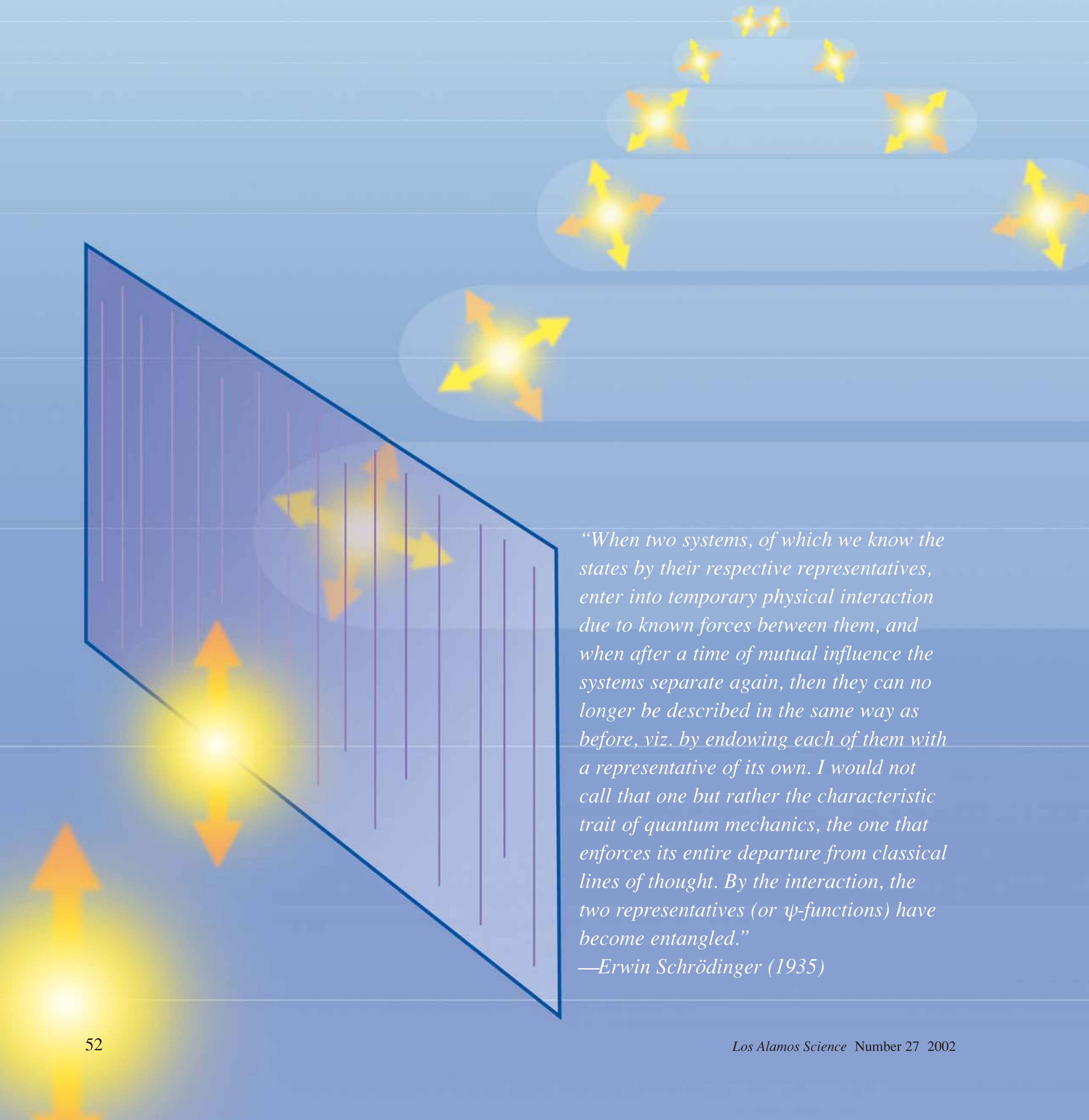


"When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction, the two representatives (or ψ-functions) have become entangled."
—Erwin Schrödinger (1935)

Quantum State Entanglement

Creation, characterization, and application

Daniel F. V. James and Paul G. Kwiat

Entanglement, a strong and inherently nonclassical correlation between two or more distinct physical systems, was described by Erwin Schrödinger, a pioneer of quantum theory, as "the characteristic trait of quantum mechanics." For many years, entangled states were relegated to being the subject of philosophical arguments or were used only in experiments aimed at investigating the fundamental foundations of physics. In the past decade, however, entangled states have become a central resource in the emerging field of quantum information science, which can be roughly defined as the application of quantum physics phenomena to the storage, communication, and processing of information.

The direct application of entangled states to quantum-based technologies, such as quantum state teleportation or quantum cryptography, is being investigated at Los Alamos National Laboratory, as well as other institutions in the United States and abroad. These new technologies offer exciting prospects for commercial applications and may have important national-security implications. Furthermore, entanglement is a sine qua non for the more ambitious technological goal of practical quantum computation.

In this article, we will describe what entanglement is, how we have created entangled quantum states of photon pairs, how entanglement can be measured, and some of its applications to quantum technologies.

Classical Correlation and Quantum State Entanglement

To describe the concept of quantum entanglement, we are first going to describe what it is not! Let us imagine the simple experiment illustrated in Figure 1. In that experiment, a source S_1 continually emits pairs of photons in two directions. As seen in the figure, one photon goes toward an observer named Alice, while the other goes toward Bob.

First, imagine that the photons emitted by S_1 are always polarized in the horizontal direction. Mathematically, we say that each photon is in the pure state denoted by the ket $|H\rangle$, that is, the "representative" of the state Schrödinger referred to in the quotation on the opposite page. Because the photons are paired, the combined state of the two photons is denoted $|HH\rangle$, where the first letter refers to Alice's photon and the second to Bob's.

Alice and Bob want to measure the polarization state of their respective photons. To do so, each uses a rotatable, linear polarizer, a device that has an intrinsic transmission axis for photons. For a given angle ϕ between the photon's polarization vector and the polarizer's transmission axis, the photon will be transmitted with a probability equal to $\cos^2\phi$. (See the box "Photons, Polarizers, and Projection" on page 76.) Formally, the polarizer acts like a quantum-mechanical projection operator P_ϕ selecting out the component of the photon wave function that lines up with the transmission axis. We say that the polarizer "collapses" the photon wave function to a definite state of polarization. If, for example, the polarizer is set to an angle θ with respect to the horizontal, then a horizontally polarized photon is either projected into the state $|\theta\rangle$ with probability $\cos^2\theta$ or absorbed with probability $1 - \cos^2\theta = \sin^2\theta$. The bizarre aspect of quantum mechanics is that the projection process is probabilistic.The fate of any given photon is completely

This article is dedicated to the memory of Professor Leonard Mandel, one of the pioneers of experimental quantum optics, whose profound scientific insights and gentlemanly bearing will be sorely missed.

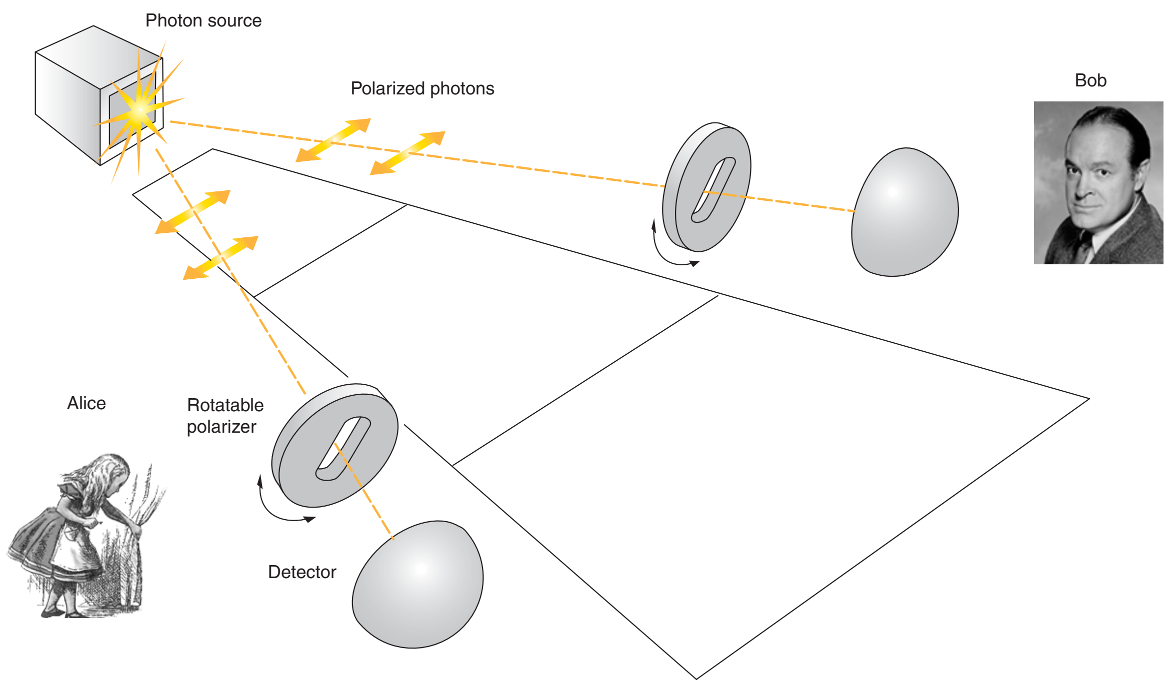


Figure 1. A Simple Two-Photon Correlation Experiment
In this experiment, a source emits pairs of photons: One photon is going to Alice and the other to Bob. Each photon passes through a linear polarizer on its way to its respective detector. Both Alice and Bob's polarizers are rotatable and can be aligned to any angle with respect to the horizontal, but Bob's is always kept parallel to Alice's. For a given polarizer setting, Alice and Bob record those instances when they have the same results, that is, when both detect photons or when they don't. The figure shows the source emitting two horizontal photons in the state $|\Psi\rangle = |HH\rangle$. The experiment can be performed with other sources to examine differences between other two-photon states. (Picture of Bob is courtesy of Hope Enterprises, Inc.)

unknown. Furthermore, any information about the photon's previous polarization state is lost.

Getting back to the experiment, we assume that Alice and Bob's polarizers are always aligned in the same way: When Alice sets her polarizer to a certain angle, she communicates her choice to Bob, who uses the same setting. Behind each polarizer is a detector. In our experiment, Alice and Bob rotate their polarizers to a certain angle with respect to the horizontal and record whether they detect a photon. Then, they repeat the procedure for different polarizer settings. If Alice looks only at her own data (or Bob looks only at his), she can determine the polarization state of the photons emitted by the source—see Figure 2(a). But Alice and Bob can also make a photon-per-photon comparison of their data and determine the probability that they have the same result, that is, they can examine the photon–photon correlations.

Suppose Alice has her polarizer oriented to transmit horizontally polarized photons. In that case, each photon coming to her from S_1 will be transmitted, and her detector will "click," indicating a photon has arrived. Subsequent communication with Bob would reveal that he also detected each photon, so at this polarizer setting, there is a perfect correlation between Alice's detection of a photon and Bob's. Similarly, by rotating the polarizer to the vertical position, the two would again discover a perfect correlation, namely, neither party would detect his or her photons.

The correlation changes when Alice and Bob have their polarizers oriented, say, at +45° to the horizontal. In that case, the photon sent to Alice has a 50 percent chance of passing through her polarizer, and independently, the photon sent to Bob has a 50 percent chance of passing through his. The probability is therefore 25 percent that both Alice and Bob detect a photon, 25 percent that neither detects a photon, and thus 50 percent that they obtain the same result.

The correlation function G is shown in Figure 2(a′). It is equal to the product of the independent probabilities for detecting a photon $[(\cos^2\theta)_A \times (\cos^2\theta)_B]$, plus the product of the probabilities for not detecting one $[(\sin^2\theta)_A \times (\sin^2\theta)_B]$, where subscripts A and B are for Alice and Bob, respectively. Thus, Alice and Bob deduce that the two photons are independent of each other and the wave function is in fact separable: $|HH\rangle = |H\rangle|H\rangle$. In other words, the correlation is entirely consistent with classical probability theory. The photons are classically correlated.

(a) S_1 emits photons in the pure state $|HH\rangle$. Alice measures a $\cos^2\theta$ function for her polarization data and deduces that photons coming to her are horizontally polarized. (A different linear polarization would shift the curve to the left or right.) (a′) We define the correlation function G as the probability that both Alice and Bob detect a photon, plus the probability that neither detects a photon. For this source, G is completely consistent with classical probability theory for independent events; that is, the correlation function is the product of the detection probability of each photon in the pair.

(b) The source S_2 emits photons in the partially mixed state $1/2(|HH\rangle\langle HH| + |VV\rangle\langle VV|)$. Photons from this source do not have a net polarization. Alice receives at random either an $|H\rangle$ or a $|V\rangle$ photon, so the sum of her measurements averages to a 50 percent detection probability independent of angle. (b′) The correlation function G, however, is the same as in (a), revealing that the photons in each pair are independent of each other and have polarization H or V. Therefore, the two photons exhibit the same classical correlations seen in (a).

(c) The source S_3 emits photons in the maximally entangled state $1/\sqrt{2}(|HH\rangle + |VV\rangle)$. Unlike the photons in the mixed state, each photon is unpolarized. Nevertheless, if Alice and Bob align their polarizers the same way, they always get the same result independent of angle. (c′) Polarization measurements of the two photons are 100 percent correlated. The photons exhibit "quantum" correlations.

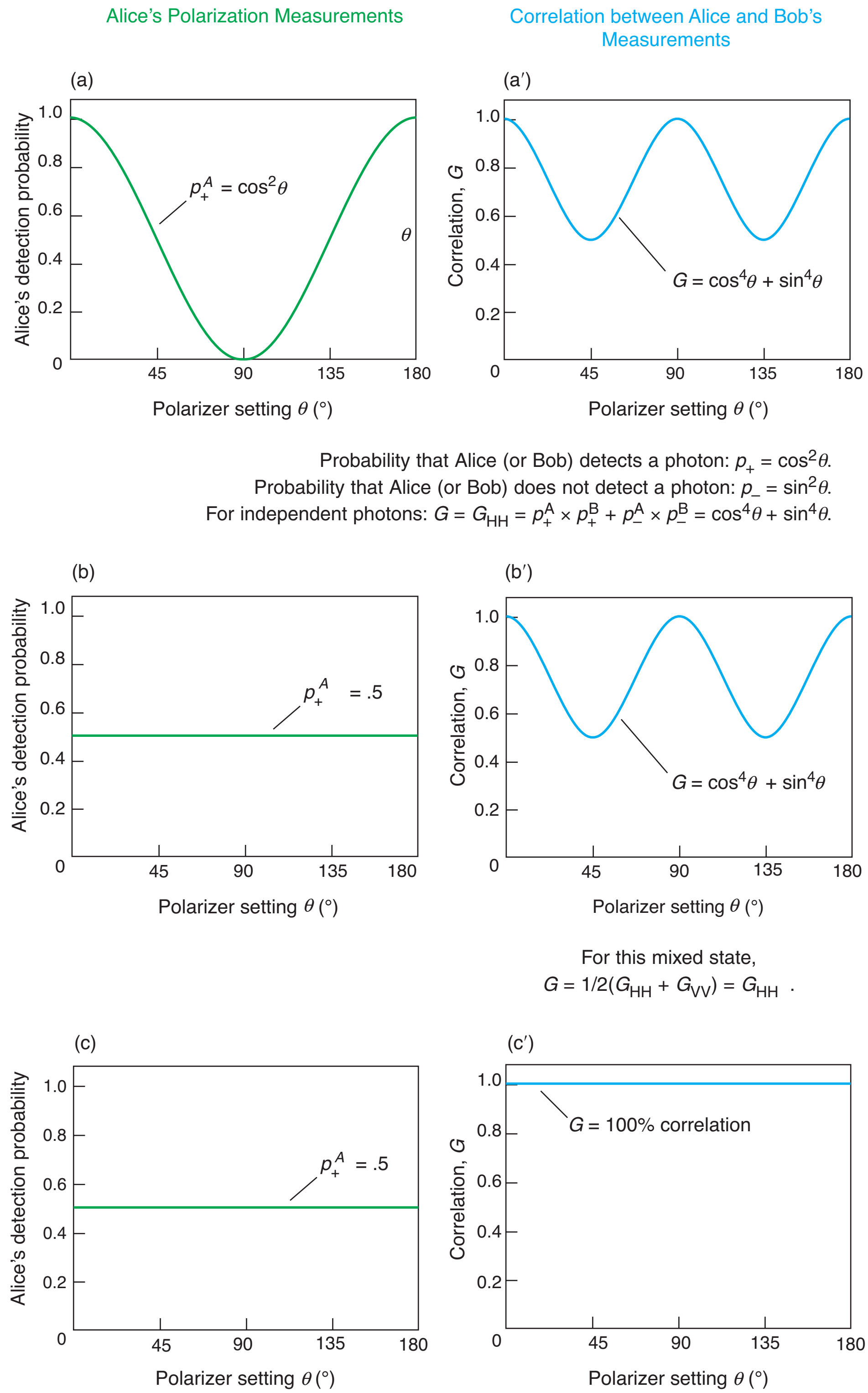


Figure 2. Quantum States, Polarization, and Correlation

The three sets of graphs show the results of the three experiments discussed in the text. In each case, the leftmost graph shows the probability that Alice alone detects a photon and reveals information about the net polarization state of her photon. The rightmost graph shows the probability that Alice and Bob have the same result, which reveals information about the two-photon state.

Pure, Entangled, or Mixed?

A pure state is a vector in a system's Hilbert space. For example, the most general, pure two-photon polarization state can be written as

$$|\psi_{\text{pure}}\rangle = \alpha|HH\rangle + \beta|HV\rangle + \gamma|VH\rangle + \delta|VV\rangle \quad . \tag{1}$$

This state is specified by the four probability amplitudes α, β, γ, and δ (expressed by four complex numbers or eight real numbers) although these parameters are subject to two constraints. The first is that the mean-square amplitudes must equal unity, that is,

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \quad . \tag{2}$$

The second relates to the fact that the overall phase of a wave function has no physical relevance. The net result of these constraints is that any pure two-photon state depends on only six independent real numbers.

In general, however, any physical system contains a greater or lesser degree of randomness and disorder, and one must adapt the formalism of quantum mechanics to take this randomness into account. We do so by averaging over the fluctuations. It is convenient to represent states as density operators, or density matrices, formally defined as

$$\rho = \overline{|\psi\rangle\langle\psi|} \quad , \tag{3}$$

where the overbar denotes an ensemble average over the randomness. All the measurable properties of the state are determined by ρ.

The density matrix must be used when representing mixed states, which can be thought of as probabilistic combinations of pure states. Mathematically, the density matrix can always be decomposed into an incoherent sum over pure states,

$$\rho = \Sigma_i p_i |\psi_i\rangle\langle\psi_i| \quad , \tag{4}$$

where each $|\psi_i\rangle$ is a pure state and p_i are probabilities with values that lie between 0 and 1 and whose sum is 1. In general, this decomposition is not unique. To characterize mixed states, one uses mean values and classical coherences; that is, one must specify the four mean-square amplitudes (subject to the constraint $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$) and the six independent classical complex correlations $\overline{\alpha^*\beta}$, $\overline{\alpha^*\gamma}$, and so on.

For example, the source S_2 mentioned in the text emits a partially mixed state that is 50 percent $|HH\rangle$ and 50 percent $|VV\rangle$, so that

$$\rho_{\text{mix}} = 0.5\,|HH\rangle\langle HH| + 0.5\,|VV\rangle\langle VV| \quad , \tag{5}$$

or in matrix form

$$\rho_{\text{mix}} = \begin{bmatrix} .5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & .5 \end{bmatrix} \quad . \tag{6}$$

This state is neither pure nor completely random; it is partially mixed.

We next consider whether quantum states involving two or more systems (for example, two photons), are separable

Now, consider performing the experiment with a second source S_2 that has a 50 percent chance to emit two horizontally polarized photons $|HH\rangle$ and a 50 percent chance to emit two vertically polarized photons $|VV\rangle$. This type of source emits photons in a mixed state, which cannot be written as a single "ket." Instead, a mixed state must be analyzed in terms of several kets, each representing a particular, distinct pure state that has a probability associated with it. Making a measurement on a mixed state is equivalent to probing an ensemble of pure states. The likelihood of measuring a particular pure state is given by the appropriate probability. (More-detailed, mathematical descriptions of pure and mixed quantum states are found in the box "Pure, Entangled, or Mixed?" above.)

The output of S_2 is random (either $|HH\rangle$ or $|VV\rangle$), so Alice receives at random either an $|H\rangle$ or a $|V\rangle$ photon. Because the probability of detecting $|H\rangle$ is 1/2 $\cos^2\theta$, and the probability of detecting $|V\rangle$ is 1/2 $\sin^2\theta$, Alice has a 50 percent chance of detecting a photon regardless of how she sets her polarizer. The same is true for Bob. Each observer, therefore, deduces that the photons coming from S_2 have no net polarization. But as seen in Figure 2(b′), the correlation function tells a different story. In fact, the correlation function for this source is identical to the one obtained for S_1 because, in both cases, the individual or entangled. If the state is separable and pure, it can be written (in some basis) as a product of the states of the individual systems, that is, as

$$|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \quad , \qquad (7)$$

where $\otimes$ denotes the tensor product. The state $|\psi_1\rangle = |HH\rangle$ is one such product of pure states and can be written as

$$|\psi_1\rangle = |H_A\rangle \otimes |H_B\rangle \quad . \qquad (8)$$

Another example is the state

$$|\psi\rangle = (|HH\rangle + |HV\rangle + |VH\rangle + |VV\rangle)/2 \quad , \qquad (9)$$

which can be written as the product state

$$|\psi\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle)_A \otimes 1/\sqrt{2}\,(|H\rangle + |V\rangle)_B \quad . \qquad (10)$$

A third example is the matrix ρ_{mix} on the opposite page, which represents a separable mixed state.

In contrast, if there is no way to write the two-photon state as a direct product of states, the state is said to be entangled. This definition leads to a quantity called concurrence, which is defined for the general pure state $|\psi_{pure}\rangle$ by

$$C = 2|\alpha\delta - \beta\gamma| \quad . \qquad (11)$$

If and only if C is zero is the state separable. If C is equal to unity (its maximum value), the state is maximally entangled.

For example, consider any one of the four Bell states

$$|\Phi_{\pm}\rangle = 1/\sqrt{2}(|HH\rangle \pm |VV\rangle) \quad \text{, and}$$

$$|\Psi_{\pm}\rangle = 1/\sqrt{2}(|HV\rangle \pm |VH\rangle) \quad . \qquad (12)$$

These states are a basis for the two-photon Hilbert space, and linear combinations of the four states can be used to represent any two-photon state. If we compare, say, $|\Phi_+\rangle$ with the general state $|\psi_{pure}\rangle$, we have $\alpha = \delta = 1/\sqrt{2}$, and $\beta = \gamma = 0$. Thus $C = 1$, and this Bell state is maximally entangled (as are the other three).

The value of C provides a good metric for the amount of entanglement in a pure two-qubit system. Equivalently, some researchers use C^2 (a quantity known as the tangle) to characterize the degree of entanglement.

The concurrence can also be defined for mixed states, although the definition is much more complicated. Indeed, calculating the concurrence for mixed states of more than two qubits is currently a hot topic of research.

In the everyday world, it is common to ascribe two (or more) variables to the same object (for example, a hot, sweet cup of coffee). Similarly, quantum states are described by the two characteristics discussed above, so that it is possible to have a pure entangled state, a pure separable state, a mixed separable state, or something in between, such as a partially mixed, partially entangled state.

photons leave the source in definite polarization states. For S_1, the polarization information is "carried" individually by each photon. For S_2, the polarization information is carried by the photon pairs. By examining the correlations, Alice and Bob can deduce that information.

A different situation occurs for a source S_3 that emits pairs of photons in the state $|\Phi_+\rangle = 1/\sqrt{2}\,(|HH\rangle + |VV\rangle)$. Like the mixed state from S_2, this state is a combination of two horizontally polarized photons and two vertically polarized photons. Unlike the mixed state, $|\Phi_+\rangle$ is a coherent, quantum mechanical superposition: A probability amplitude is associated with each component, $|HH\rangle$ and $|VV\rangle$, and the two components have a fixed phase relationship. An important property of this particular state is that we can rotate the axes of polarization (H and V) and not change the state's essential properties.

The state $|\Phi_+\rangle$ is a fully entangled quantum state. It cannot be factorized, or separated, into a part describing one of the photons and a part describing the other. The two photons are inextricably linked to each other and their properties are always correlated. A measurement of one of the photons makes the two-photon state instantly disappear, and the remaining photon assumes a definite state that is perfectly correlated with the measured photon. Neither photon carries definite information by itself—all the information is carried in the joint two-photon state.

Thus, when Alice and Bob repeat the experiment using the source S_3, the correlation is 100 percent regardless of polarizer orientation (assuming Bob's polarizer is always set the same way as Alice's). Figure 2(c) illustrates the striking difference between the classical correlations of the photons generated by the sources S_1 and S_2 and the nonclassical correlations exhibited by entangled photons.

To better understand the correlation curve shown for $|\Phi_+\rangle$, consider that quantum mechanics allows us to express that state in any basis; that is, $|\Phi_+\rangle = 1/\sqrt{2}\,(|XX\rangle + |YY\rangle)$, where $|X\rangle$ is an arbitrary linear-basis state and $|Y\rangle$ is the orthogonal-basis state. Suppose Alice has her polarizer set to +45°. In the diagonal (+45/–45) basis, the entangled state will be $|\Phi_+\rangle = 1/\sqrt{2}\,(|{+45},{+45}\rangle + |{-45},{-45}\rangle)$. If Alice detects her photon (a 50–50 proposition), then Bob's photon will collapse to the $|{+45}\rangle$ state, and he will detect his photon as well. Likewise, if Alice doesn't detect her photon, Bob won't detect his. The same deductions can be made for any polarizer setting.

According to quantum mechanics, the correlation occurs regardless of the distance separating the two photons. For example, suppose one of two entangled photons from the state $|\Phi_+\rangle$ is sent to Alice, who "stores" it in her laboratory at Los Alamos, New Mexico. The other photon is sent to Bob, who is in orbit about the star α-Centauri, nearly 4 light-years away. After some time, Alice performs a measurement on her photon and determines that it is $|H\rangle$. Her measurement selects the $|HH\rangle$ part of the state $|\Phi_+\rangle$ and eliminates the $|VV\rangle$ part so that Bob's photon is necessarily in the state $|H\rangle$. If, instead, Alice has determined that her photon was $|{+45}\rangle$, the state of Bob's photon will be instantly collapsed to $|{+45}\rangle$ as well. In other words, the state of Bob's photon has been nonlocally influenced by Alice's measurement. By nonlocal, we mean that the correlation between Alice and Bob's measurements occurs even if there is not enough time for a light signal (or any signal) to propagate between the two experimentalists. This is not to say that special relativity has been violated: Because Alice cannot predetermine the outcome of her measurement, she cannot use the nonlocal quantum correlations to send any information to Bob. In fact, entanglement can never be used to send signals faster than the speed of light. Nonetheless, Bob's photon "knows" the outcome of Alice's measurement.

Nonlocality was the central point of a famous argument raised by Albert Einstein, Boris Podolsky, and Nathan Rosen in 1935, now known as the EPR paradox. The three physicists disagreed with the Copenhagen interpretation of quantum mechanics, according to which the state of a quantum system is indeterminate until it is projected into a definite state as a result of a measurement. Einstein, Podolsky, and Rosen argued that even unmeasured quantities corresponded to definite "elements of reality." The quantum state only appeared to be indeterminate because some of the parameters that characterize the system were unknown and unmeasurable. These local parameters, or "hidden variables," determined the outcome of the experiment.

In 1964, John Bell showed that the correlations between measured properties of any classical two-particle system would obey a mathematical inequality, but the same measured correlations would violate the inequality if the two particles were an entangled quantum system. Experiments could therefore determine if nature exhibited nonlocal features. Following the development of laboratory sources of entangled photons, experimental tests of Bell's inequality were pursued with vigor. The results to date suggest that the observed photon correlations cannot be explained by any local hidden-variable theory,[1] and most physicists agree that quantum mechanics is truly a nonlocal theory.

Entanglement and Quantum Information

Entanglement, a measurable property of quantum systems, can be exploited for specific goals. Here, we present three potential applications, all of which have been shown to work as proof-of-principle demonstrations in the laboratory.

Quantum Cryptography. Consider two bank managers, Alice and Bob, who want to have a secret conversation. If they are together in the same room, they can simply whisper discretely to each other, but when Alice and Bob are in their respective cross-town offices, their best chance for secret communication is to encrypt their messages.

A generic, classical encryption protocol would begin when Alice and Bob convert their messages to separate binary streams of 0s and 1s. Encryption (locking up the messages) and decryption (unlocking the messages) are then performed with a set of secret "keys" known only to the two bankers. Each key is a random string of 0s and 1s that is as long as the binary string comprising each

[1] There were two loopholes to the EPR tests. The first stemmed from the fact that the detectors were not efficient enough. Consequently, the observed correlations could have been the result of some new physics that did not require nonlocal interactions. The second loophole stemmed from the researchers' inability to choose rapidly and randomly a basis for photon measurement. This inability allowed for a potential communication conspiracy between Alice and Bob's systems. Both of these loopholes have recently been closed but, so far, not in the same experiment.

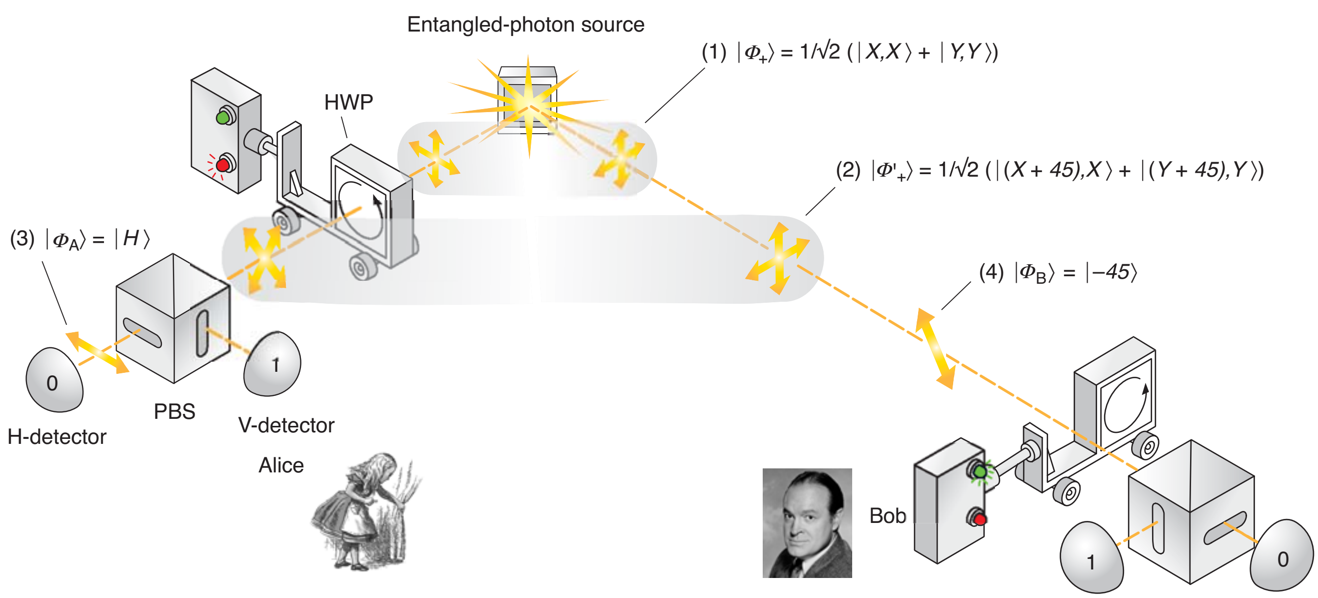


Figure 3. Quantum Cryptography Using Entangled Photons

Alice and Bob can use the properties of entangled photons to create a pair of identical cryptographic keys. (1) The source emits entangled photons in a maximally entangled state $|\Phi\rangle = 1/\sqrt{2}(|XX\rangle + |YY\rangle)$, where $|X\rangle$ is an arbitrary linear-basis state and $|Y\rangle = |X + 90\rangle$ is the orthogonal-basis state. One photon goes to Alice and the other to Bob. (2) Alice chooses at random either to let her photon pass or to insert a half-wave plate (HWP), which will rotate her photon by +45°. The latter choice changes the relative orientation between the two photons by +45°. In the case shown, she chooses to rotate her photon. The new entangled state is $|\Phi'\rangle$. (3) Alice uses a polarizing beam splitter (PBS) to measure her photon in the H/V basis. This optical element transmits horizontally polarized photons and reflects vertically polarized photons, and her unpolarized photon can collapse to either a horizontal or vertical polarization with equal probability. In this case, it collapses to a horizontal polarization. Alice records a bit value of 0. (5) Bob's photon was entangled with Alice's, so as a result of her measurement, his photon assumed the definite polarization state $|H - 45\rangle = |-45\rangle$. If Bob makes the same choice as Alice and inserts his HWP, he will rotate his photon's polarization by +45° and into a horizontal polarization. His photon will register in the H-detector, and he will record a bit value of 0. If he makes the opposite choice and doesn't rotate his photon, the photon polarized at –45° has an equal probability of going to either detector (bit value either 0 or 1). As seen in Table I on the next page, whenever Bob and Alice make the same choice, they keep the bit because their bit values coincide. If they make opposite choices, they discard the bit since the values are not correlated. Alice and Bob can construct an identical sequence of random bits—a cryptographic key—simply by declaring their sequence of choices. The discussion can be public because the bit values are never revealed.

message. To encrypt, Alice (the sender) sequentially adds each bit of the key to each bit of her message, using modulo 2 addition (0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, and 1 + 1 = 0). She then sends the encrypted message to Bob, who decrypts it simply by repeating the operation, that is, by performing a sequential, bit-by-bit modulo 2 addition of the key to the message.

This type of encryption protocol, known as a one-time pad, is currently the only provably secure protocol. But the one-time pad is effective only if Alice and Bob never reuse the key, and more obviously, if the key remains secret. A potential eavesdropper, Eve, cannot be allowed to glean any part of the bit stream that makes up the key. Therein lies a central problem of cryptography: How can secret keys be created and then securely distributed? The nonlocal correlations of entangled photons can play a role in this regard. (One can also exploit the properties of nonentangled photons in cryptographic schemes. See the article "Quantum Cryptography" on page 68.)

In the entangled-state quantum cryptography scheme, Alice and Bob perform an experiment similar to the one described in the first section of the paper. They use a source S_3 that emits entangled photons in the general state $|\Phi_+\rangle = 1/\sqrt{2}\,(|XX\rangle + |YY\rangle)$, where $|X\rangle$ is an arbitrary linear-basis state and $|Y\rangle$ is the orthogonal-basis state. One photon goes to Alice and the other to Bob. In this protocol, however, either banker can choose—at random and independent of each other—to use a half-wave plate (HWP) to rotate photon polarization by a set amount. The bankers then detect the photon in the H/V basis using a polarizing beam splitter, which transmits horizontally polarized photons and reflects vertically polarized photons (see Figure 3).

Table I. Constructing a Cryptographic Key with Entangled Photons

First Receiver (Alice)			Polarization to Second Receiver	Second Receiver (Bob)			Communication Results
Angle of Rotation (°)	Detector	Bit Value		Angle of Rotation (°)	Detector	Bit Value	
0	H	0	H	0	H	0	Keep bit
0	V	1	V	0	V	1	Keep bit
0	H	0	H	+45	H or V	0 or 1	Discard bit
0	V	1	V	+45	H or V	0 or 1	Discard bit
+45	H	0	–45°	0	H or V	0 or 1	Discard bit
+45	V	1	+45°	0	H or V	0 or 1	Discard bit
+45	H	0	–45°	+45	H	0	Keep bit
+45	V	1	+45°	+45	V	1	Keep bit

Detection of a horizontally polarized photon is recorded as a 0; of a vertically polarized photon, as a 1.

After a sufficient number of measurements (that number is dictated by the length of the key), Alice and Bob have a public discussion, during which they reveal whether they inserted the HWP before each measurement. At no time do they reveal the actual measurement results. Whenever Alice and Bob make the same choice (50 percent of the time), they know from the properties of entangled photons that they will have completely correlated results. By contrast, if one of them uses the HWP and the other doesn't, they will discard the results because their measurements would be completely uncorrelated (see Table I). Following this public discussion, each banker will be able to privately construct the same random string of 0s and 1s—an ideal key for cryptography.

What about the eavesdropper Eve? She is completely foiled in her attempts to know the secret key. Certainly, she cannot tap the photon line, as she might with conventional, classical communications. A single, indivisible quantum object—namely, a photon—is the conveyor of information in this cryptographic protocol. If Eve steals Bob's photon (a "denial-of-service" attack), the photon's information never becomes part of the key. Thus, although a wiretap would reduce the rate of the transmission, it would not jeopardize the security of the key.

Eve can try to intercept the photon, measure it, and send another one to Bob. But any measurement Eve would make to determine the photon's polarization state would necessarily perturb the photon and collapse the entangled state. The photon she sends to Bob would therefore be classically correlated with Alice's photon. Consequently, Eve's intervention would necessarily induce additional errors into Bob's key.

This last point is significant. Unlike their theoretical counterparts, the encryption keys created by an actual quantum cryptography system initially have a small fraction of errors, because real equipment is always less than perfect. To make sure their key is secure, Alice and Bob ascribe all errors to Eve and then use this "bit error rate" to estimate the maximum amount of information available to the eavesdropper. They then use a privacy amplification scheme (discussed in the cryptography article on page 68) to reduce Eve's knowledge of the secret key to less than one bit.

But the bit error rate alone can lead to a false sense of security. If nonentangled photons with a definite polarization are sent to Bob, it is conceivable that some other degree of freedom may also be coupled to the polarization state. For example, if separate lasers are used to produce the two polarization states, the photons from each laser may have slightly different timing characteristics or frequency spectra. Such a difference would in principle allow an eavesdropper to distinguish between photons without disturbing the polarization state and, hence, without affecting the bit error rate.

When the photons are entangled, however, any leakage of information to other degrees of freedom can be shown to automatically manifest itself in the error rate detected by Alice and Bob. In other words, any degree of freedom with which the polarization might be coupled will cause noticeable effects on the polarization correlations. Therefore, using only the detected error rates, one can set an upper limit on the information available to an eavesdropper, even one who is not directly measuring the polarization of the photons, and then use privacy amplification to eliminate that information.

As a last resort, Eve may think of "cloning" Alice's photon. She could measure the clone while allowing the

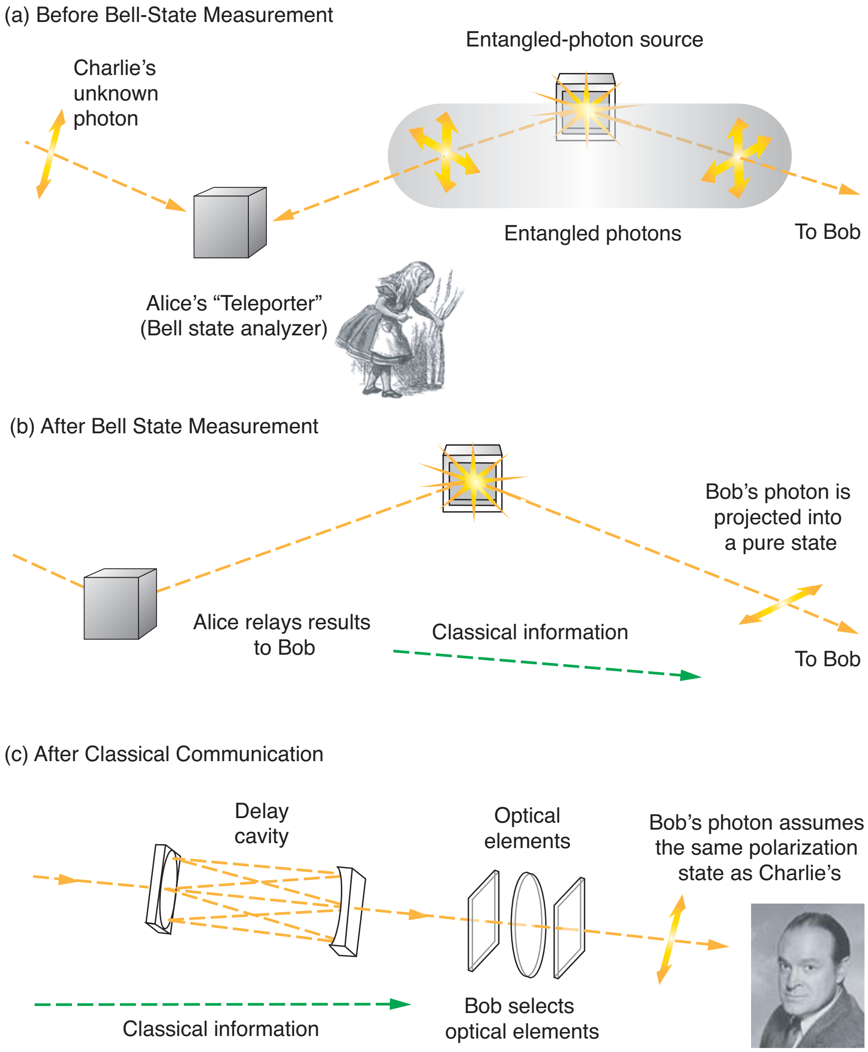


Figure 4. Quantum State Teleportation
(a) Alice's teleportation lab consists of an entangled photon source and a Bell state analyzer (the teleporter). One entangled photon goes to Bob and the other to the teleporter. Charlie sends a photon of unknown polarization state into the teleporter. (b) Alice performs a joint polarization measurement of the two photons in the teleporter and relays the result to Bob using two classical bits of information. The photon going to Bob is projected into a pure state as a result of Alice's measurement. (c) Upon receiving Alice's classical information, Bob performs a simple transformation on his photon, such as a rotation of the polarization vector. He duplicates the polarization state of Charlie's photon without knowing anything about its original state.

original to continue on to Bob, thus completely covering her tracks. But she is again foiled by quantum mechanics. According to the no-cloning theorem, it is impossible to make a copy of a photon in an unknown state while simultaneously preserving the original. (See the box "The No-Cloning Theorem" on page 79.) Eve is clearly out of business.

Teleportation. In 1993, Charles Bennett of IBM, Yorktown Heights, and his colleagues proposed a remarkable experiment with entangled particles, namely, the "teleportation" of a pure quantum state from one location to another.

Charlie wants to send his friend Bob a photon in an arbitrary, pure quantum state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$. He enlists the aid of Alice, who happens to run the Teleportation Laboratory shown in Figure 4. Inside the lab, a source S_3 is emitting a pair of entangled photons, one of which goes off to Bob. The other photon is input into Alice's "teleporter." Charlie is instructed to send his photon into the teleporter as well.

Alice then performs a special joint measurement of the polarization state of the two photons in the teleporter. She relays the result to Bob, who subsequently performs a simple transformation of the polarization state of his photon. As if by magic, the state of Bob's photon is transformed into the state of Charlie's original photon.

Mathematically, this magic is described as follows. The three-photon initial state (that is, Charlie's photon plus the two entangled photons) can be represented as

$$|\psi_0\rangle = (\alpha|H\rangle + \beta|V\rangle)_C \times 1/\sqrt{2}(|HH\rangle + |VV\rangle)_{A,B} \ , \quad (1)$$

where the subscripts C, A, and B refer to Charlie's, Alice's, and Bob's photons, respectively. But $|\psi_0\rangle$ can also be represented as a superposition of states, each constructed in the following way: Charlie and Alice's photons are represented by one of the Bell states $|\Phi_{\pm}\rangle = 1/\sqrt{2}\,(|HH\rangle \pm |VV\rangle)$ and $|\psi_{\pm}\rangle = 1/\sqrt{2}(|HV\rangle \pm |VH\rangle)$,

and Bob's photon is represented as a photon in a pure state. Thus,

$$
\begin{aligned}
|\psi_0\rangle = 1/2\{ & |\Phi_{-}\rangle_{C,A}\,(\alpha|H\rangle - \beta|V\rangle)_B \\
& + |\Phi_{+}\rangle_{C,A}\,(\alpha|H\rangle + \beta|V\rangle)_B \\
& + |\Psi_{-}\rangle_{C,A}\,(-\beta|H\rangle + \alpha|V\rangle)_B \\
& + |\Psi_{+}\rangle_{C,A}\,(\beta|H\rangle + \alpha|V\rangle)_B \} \quad . \qquad (2)
\end{aligned}
$$

Technically speaking, this representation is possible because the Bell states are a basis for the two-photon Hilbert space and any state of two photons can be represented as a linear superposition of these states. It is important to point out that Alice's photon remains entangled with Bob's. Teleportation relies on Alice's ability to perform a joint polarization measurement that explicitly projects the two photons in the teleporter into one of the four Bell states. Once Alice completes her measurement, Bob's photon (which is totally correlated to Alice's) will assume the corresponding pure state. For example, if the Bell state measurement produces the result $|\Psi_{-}\rangle_{C,A}$, then Bob's photon would be projected into the pure state $|\psi\rangle = (-\beta|H\rangle + \alpha|V\rangle)_B$. By using a simple optical element, Bob can rotate the polarization state of his photon by 90° and transform it into the state $|\psi'\rangle = (\alpha|H\rangle + \beta|V\rangle)_B$, that is, the original input state. Provided Alice can specify which Bell state was measured (a specification that requires two bits of classical information), Bob can always choose an appropriate optical element to effect the proper rotation.

In a series of groundbreaking experiments conducted at the University of Innsbruck, Austria, Anton Zeilinger and coworkers were the first to demonstrate quantum teleportation. The group is now able to determine two of the four Bell states unambiguously (the other two states give the same experimental signature[2]) and prove for those cases that the state of Charlie's photon could indeed be transferred to Bob's.

Several points should be made about quantum teleportation. First, during the entire procedure, neither Alice nor Bob has any idea what the values are for the parameters α and β that specify Charlie's photon. The initial, arbitrary pure state remains unknown. Second, teleportation is not cloning. The original state of Charlie's photon is necessarily destroyed by Alice's measurement, so the photon that Bob ends up with is still one of a kind.

Finally, hopeful sci-fi fans may be a little disappointed by this realization of teleportation. Unlike the TV show "Star Trek," in which Captain Kirk could be transported body and soul from the starship *Enterprise* to the surface of an alien planet,[3] here only certain information about the photon is transferred to a photon in some faraway location. Because photons have numerous degrees of freedom in addition to their polarization, the original and the teleported photons are two different entities. And it goes without saying that an even simpler way for Charlie to send his quantum state to Bob would be to dispatch the original photon directly to him.

Nevertheless, teleportation remains an interesting application of quantum state entanglement. Furthermore, researchers have discussed how it might form the basis of a distributed network of quantum communication channels and how this basic information protocol might be useful for quantum computing.

Quantum Microscopy and Lithography. The general topic of quantum metrology involves capitalizing on the ultrastrong correlations of entangled systems to make measurements more precisely than would be possible with classical tools. The two main photon-based applications under investigation are quantum microscopy and quantum lithography.

At present, two-photon microscopy is widely used to produce high-resolution images, often of biological systems. However, the classical light sources (lasers) used for the imaging have random spreads in the temporal and spatial distributions of the photons, and the light intensity must be very high if two photons are to intersect within a small enough volume and cause a detectable excitation. The high intensity can damage the system under investigation. Because the temporal and spatial correlations may be much stronger between members of an entangled photon pair, one could conceivably get away with much weaker light sources, which would be much less damaging to the systems being observed. Moreover, entangled-photon sources may also enable obtaining enhanced spatial resolution.

Lithography, in which a pattern is optically imaged onto some photoresist material, is the primary method of manufacturing microscale or nanoscale electronic devices. An inherent limitation of this process is that details smaller than a wavelength of light cannot be written reliably. However, quantum state entanglement might circumvent this limitation. Under the right circumstances, the interference pattern formed by beams of entangled photon pairs can have half the classical fringe spacing.

Quantum lithography requires two beams of photons, which we

[2] Distinguishing between the four Bell states is still an unsolved technical problem. It requires a strong nonlinear interaction between two photons, which is extremely difficult to achieve in practice.

[3] "Teleportation" (though it was not explicitly called that) was supposedly introduced in this TV show because the producer, Gene Roddenberry, wished to save the expense of simulating the landing of a starship on a planet.

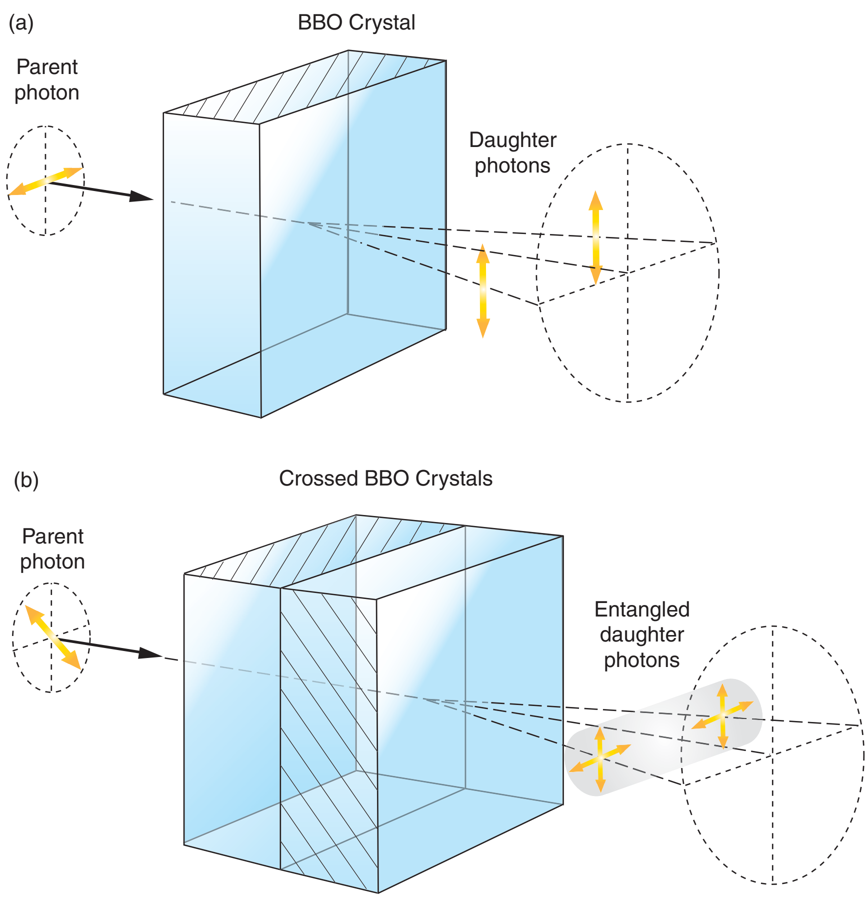


Figure 5. Entangled-Photon Source
(a) For a given orientation of the beta-barium borate (BBO) crystal, a horizontally polarized parent photon produces a pair of vertically polarized daughters. The daughters emerge on opposite sides of an imaginary cone. The cone's axis is parallel to the original direction taken by the parent photon. The two daughter photons are not in an entangled state. Reorienting the BBO crystal by 90° will produce a pair of horizontally polarized daughters if a vertically polarized pump beam is used. (b) Passing a photon polarized at +45° through two crossed BBO crystals can produce two photons in an entangled state. Because of the Heisenberg uncertainty principle, there is no way to tell in which crystal the parent photon "gave birth," and so a coherent superposition of two possible outcomes results: a pair of vertically polarized photons or a pair of horizontally polarized photons. The photons are in the maximally entangled state $|\Phi_+\rangle = 1/\sqrt{2}(|HH\rangle + |VV\rangle)$.

will call A and B, but in this case, the type of entanglement is different from the one discussed in the previous sections. What is needed is a coherent superposition consisting of the state in which two photons are in beam A while none are in B and the state in which no photon is in beam A while two photons are in B. Such number-entangled states can be made in the laboratory, and the predictions about fringe spacings have been verified. However, other obstacles must be overcome in order to surpass current classical-lithography techniques. Researchers continue to explore the potential of this ideawith the hope of achieving a viable commercial technology.

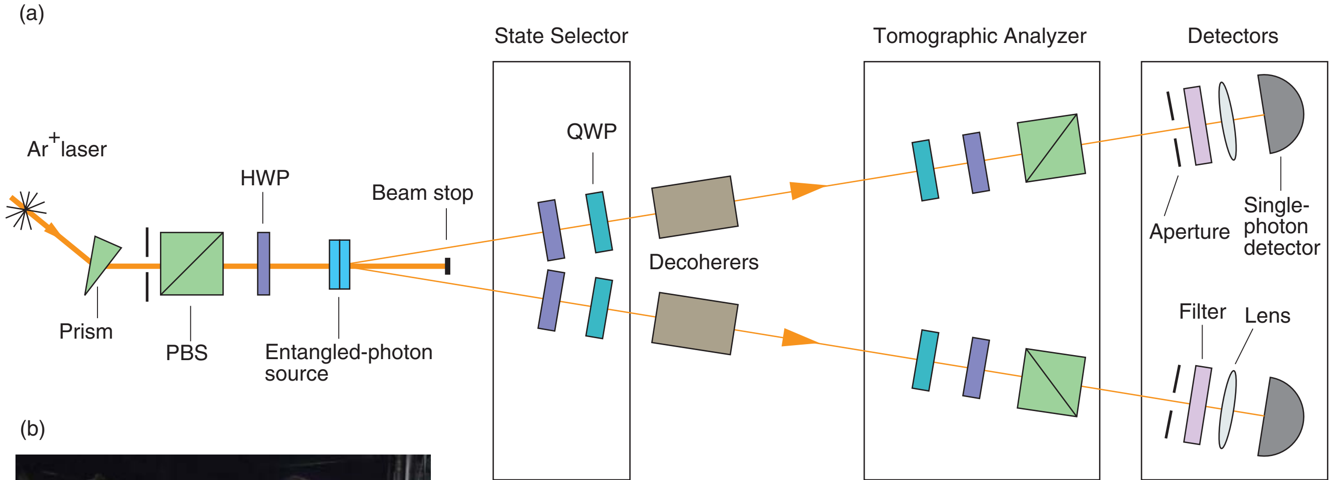
Creating and Measuring Entangled States

If quantum state entanglement is such a remarkable property because it allows one to perform secret communications, teleport states, or test the nonlocality of quantum mechanics, one naturally wonders how to make entangled states. Currently, scientists can create entangled states of particles in a controlled manner by using several technologies such as ion traps, cavity quantum electrodynamics (QED), and optical down-conversion. Here, we will concentrate on the optical realization.

Crystals of a certain chemical structure, such as beta-barium borate (BBO), have the property of optical nonlinearity, which means that the polarizability of these crystals depends on the square (or higher powers) of an applied electric field. The practical upshot of this property is that, when passing through such a crystal, a single-parent photon can split (or down-convert) into a pair of daughter photons. The probability that this event occurs is extremely small; on average, it happens to only one out of every 10 billion photons!

When down-conversion does occur, energy and momentum are conserved (as they must be for an isolated system). The daughter photons have lower frequencies (longer wavelengths) than the parent photon and emerge from the crystal on opposite sides of a cone that is centered about the direction traveled by the parent. For what is known as Type I phase matching, the daughters emerge from a specifically oriented BBO crystal with identical polarizations that are aligned perpendicular

(a)



(b)

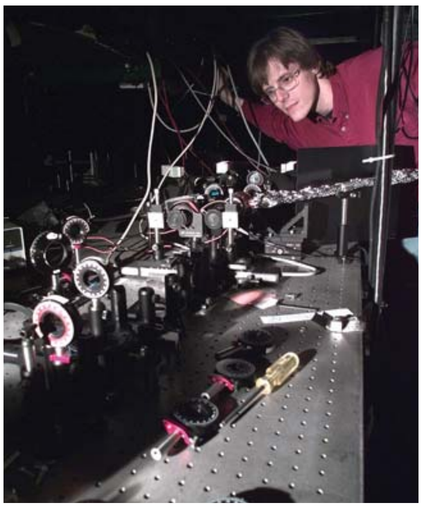


Figure 6. Creating and Measuring Two-Photon Entangled States
(a) The "parent" photons are created in an argon ion laser and are linearly polarized with a polarizing beam splitter (PBS). The half-wave plate (HWP) rotates the polarization state before the photon enters the entangled-photon source. The entangled photons produced diverge as they exit. Each photon's polarization state can be altered at will by the subsequent HWP and quarter-wave plate (QWP). The decoherers following the state selection allow us to produce (partially) mixed photon states. The optical elements (QWP, HWP, and PBS) in the tomographic analyzer allow us to measure each photon in an arbitrary basis, for example in H/V or +45/–45. Combining the measurements on both photons allows us to determine the quantum state. (b) In the photo, Paul Kwiat is shown with the two-photon entangled source at Los Alamos.

to the parent polarization—see Figure 5(a). Because each photon is in a definite state of polarization, the two photons are not in an entangled state but are classically correlated. (The crystal acts like the source S_1 described earlier.)

To create photons in the entangled state, one can use two crystals that are aligned with their axes of symmetry oriented at 90° to each other, as shown in Figure 5(b). With crossed crystals, two competing processes are possible: The parent photon can down-convert in the first crystal to yield two vertically polarized photons ($|VV\rangle$), or it can down-convert in the second to yield two horizontally polarized photons ($|HH\rangle$). It is impossible to distinguish which of these processes has occurred. Thus, the state of the daughter photons is a coherent quantum-mechanical superposition of the states that would arise from each crystal alone; the crossed crystals produce photons in the state $|\Psi_{out}\rangle = 1/\sqrt{2}(|HH\rangle + |VV\rangle)$, which is maximally entangled.[4]

Figure 6 shows how this basic source can be adapted to produce any pure quantum state of two photons by placing rotatable half- and quarter-wave plates (which can be used to transform the polarization state of a single photon) before the crystal and in the paths of the two daughter photons. To create more general quantum states—mixed states—a long birefringent crystal can be used to delay one polarization component with respect to the other. If the relative delay is longer than the coherence time of the photons, the horizontal and vertical components have been effectively decohered; that is, the phase relationship between the different states is destroyed. Researchers are still discovering how to combine sources and polarization-transforming elements to create all possible two-photon quantum states.

[4] In an alternative approach known as "Type II phase matching," only one crystal is needed to create the entangled state. The crystal has a different orientation, and each of the daughter photons emerges from the crystal on one of two possible exit cones. Entangled photons created by this approach were used in the first demonstration of quantum teleportation.

Characterizing Entanglement:

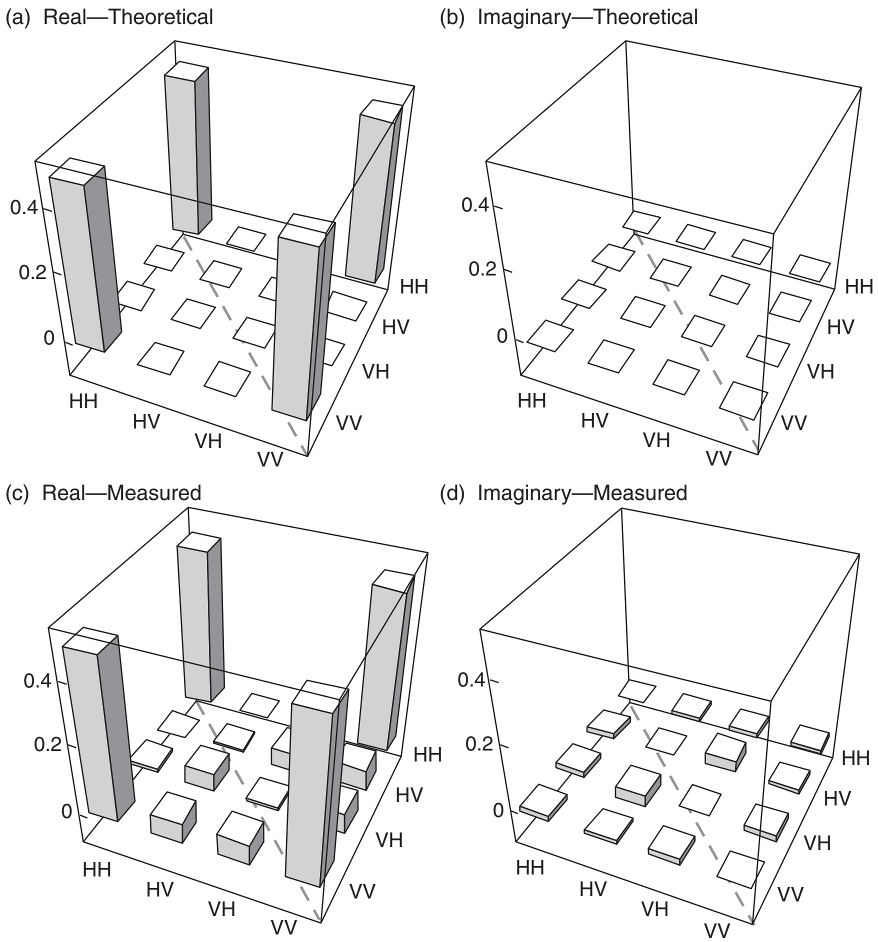


Figure 7. Density Matrices
Theoretical and experimental density matrices for the entangled state $|\Phi_+\rangle = 1/\sqrt{2}\,(|HH\rangle + |VV\rangle)$ are illustrated here. Both real and imaginary parts of the matrix are shown. The value of each matrix element is derived from the results of thousands of two-photon correlation experiments (simulated experiments for the theoretical matrix.) The experimental matrix indicates that our source can output a state close to a maximally entangled one. Written out "longhand," the density matrix describing the state $|\Phi_+\rangle$ is

$$\rho = |\Phi_+\rangle\langle\Phi_+| = 1/2(\,|HH\rangle\langle HH| + |VV\rangle\langle VV| + |HH\rangle\langle VV| + |VV\rangle\langle HH|\,)\ .$$

The first two terms, which lie on the diagonal of the matrix (dashed line), give the probability of the result (for example, 50% HH and 50% VV). The other two terms describe the quantum coherence between the states $|HH\rangle$ and $|VV\rangle$. For a classical mixed state (such as the source S_2 described in the text), these off-diagonal terms in the density matrix would equal zero. Notice that all coefficients in this density matrix are real, so that all terms in the imaginary part of the matrix should be zero.

The Map of Hilbert Space

As discussed in the box on page 56, a mixed state of two photons (or in general, a mixed state of two qubits) is represented by a 4 × 4 density matrix, which is described by 15 independent parameters (15 real numbers). To determine the independent parameters, we make 15 coincidence measurements on the ensemble of photon pairs emitted from the source. Each measurement is similar to the one used in the simple experiment described at the start of this article. The measurement may be made with the tomographic analyzer shown in Figure 6. Using such a system, we were able to determine the density matrices of many types of states. An example is shown in Figure 7.

Whereas 15 numbers fully describe a two-photon mixed state, the density matrix for N photons needs $4^N - 1$ real numbers. Thus, the density matrix of a 4-photon state contains 255 parameters and requires 255 separate measurements just to characterize the state. Note that, if each parameter is allowed to assume one of, say, 10 possible values, those 4 photons can be in any of 10^{255} distinct quantum states! This number of states is many orders of magnitude greater than the total number of particles in our universe. The mathematical space in which the quantum states rest (the Hilbert space) is unfathomably large, and in order to have any hope of navigating it, one needs to introduce a simpler representation for quantum states.

Two characteristics of central importance for quantum information processing are the extent of entanglement and the degree of purity of an arbitrary state. A quantity called the von Neumann entropy has been introduced to characterize the degree of purity. (See the box "Characterizing Mixed States" on the next page.) However, for the analysis of two-photon states, we found it easier to use a related quantity, known as the linear entropy. When the linear entropy equals zero, the state is pure. When it reaches its maximum value of 1, the state is completely random.

Measuring the entanglement of a mixed state is more complicated and, in general, is an unsolved research problem when more than two qubits

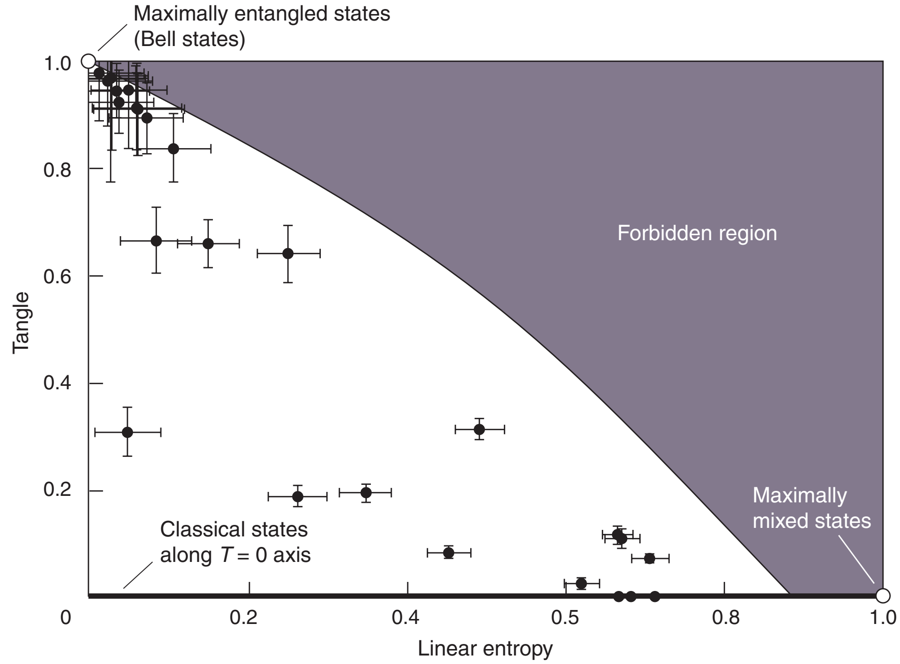


Figure 8. The Map of Hilbert Space
The amount of entanglement (or the tangle) is plotted against the degree of purity (represented by the linear entropy) for a multitude of two-photon states created and measured at Los Alamos. Each state is represented by a black spot with error bars. The boundary line, which represents the class of states that have the maximum possible entanglement for a given value of the linear entropy, was first determined theoretically but then confirmed by a numerical simulation of two million random density matrices. Important states, such as those that are maximally entangled or completely mixed, are indicated. Efforts are under way to create states that lie along the boundary line.

are involved. Any mixed quantum state can be thought of as an incoherent combination of pure states: The system is in a number of possible pure states, each of which has some probability between 0 and 1 associated with it (rather than the complex numbers defining the probability amplitudes that specify a particular superposition of pure states). A reasonable measure of the entanglement of such a mixed state is to take the average value of the entanglement (for example, as measured by the concurrence discussed in the box on this page) for all those pure states.

One must, however, use this procedure carefully because the decomposition of the mixed state into an incoherent sum of pure states is not unique. For this "average entanglement" to make any sense as a measure of entanglement of the mixed state, one must use the decomposition for which the average is a minimum. The square of this minimized quantity is called the "tangle." It has a value of zero for entirely unentangled, separable states and of unity for completely entangled states.

Figure 8 shows how those two

Characterizing Mixed States

It is convenient to characterize the extent of entanglement and the degree of purity of a mixed state using two derived parameters: the tangle and the linear entropy. The linear entropy, which gives a measure of the purity of the state, derives from the von Neumann entropy. The latter is given by the formula $S = -\mathrm{Tr}\{\rho \log_2(\rho)\}$, where ρ is the density matrix. Here Tr{M} is the trace of a matrix (that is, the sum of terms on the diagonal) and $\log_2$ is a logarithm base 2, which can be defined for matrices via a power series. The von Neumann entropy is zero for a pure state. When the von Neumann entropy has its maximum value (equal to the number of qubits), the state is completely random, with no information or entanglement being present. The linear entropy, defined for two qubits as $S_L = 4/3(1 - \mathrm{Tr}\{\rho^2\})$, is similar to the von Neumann entropy, but it is easier to calculate. Specifically, it equals 0 for a pure state and has a maximum value of 1 for completely random states.

Characterizing the degree of entanglement is more difficult. Mathematically speaking, if one decomposes the density matrix into an incoherent sum of pure states, that is, $\rho = \Sigma_i\, p_i\, |\psi_i\rangle\langle\psi_i|$, where $0 \le p_i \le 1$ and $\sum_i p_i = 1$, then the average entanglement is $\bar{E} = \sum_i p_i C(\psi_i) = 1$, where $C(\psi_i)$ is the concurrence of the pure state $|\psi_i\rangle$ (defined in the box on page 56). It is very important to find the decomposition for which $\bar{E}$ takes its minimum possible value; otherwise, one can infer a nonzero entanglement for states such as the completely mixed state, which is certainly not entangled! Fortunately, the way to do that decomposition has been worked out for two qubits. Characterizing the degree of entanglement for three or more qubits remains an unsolved research problem.

parameters—tangle and linear entropy—can be used to create a simplified map of Hilbert space for two-photon states. The crosses (with error bars) are the states we have created and measured experimentally. Most display a high degree of entanglement. States created by other technologies can be plotted on such a diagram as well.

Conclusions

Entangled states arise naturally whenever two or more quantum systems interact. In fact, one of the prevalent theories of nature is that the universe is really one big, vastly complicated entangled state, described by the "wave function of the universe." Despite their seeming ubiquity, however, entangled states are not generally observed in the world at large. Only relatively recently have scientists developed the means to controllably produce, manipulate, and detect this most bizarre quantum phenomenon. Initially, the fascination was limited to experimental studies of the foundations of quantum mechanics, especially the notion of nonlocal "spooklike" influences (to quote Einstein). However, even more recently, has come the realization that entanglement could lead to enhanced—sometimes vastly enhanced—capabilities in the realm of information processing.

This paper has discussed how entangled states could be a key resource in applications as diverse as cryptography, lithography, and metrology because they enable feats beyond those possible with classical physics. In addition, the quest to create a quantum computer has pushed entangled systems to the forefront of quantum research. Part of the power of a quantum computer is that it creates entangled states of N qubits so that information can be stored and processed in the 2^N-dimensional qubit space. Quantum algorithms have been developed that would manipulate the complex entangled state and make use of the nonclassical correlations to solve problems more efficiently than could be done classically. Scientists who work on developing quantum computers are envisioning systems of thousands of entangled qubits.

We don't know whether we will be able to create or maintain such a complex entangled state. At this point, we won't even claim to know whether we will fully understand that state if it is created. More research is needed before those questions can be answered. All that we can say now is that the once-hidden domain of quantum entanglement has broken into our classical world. ■

Further Reading

Bouwmeester, D., A. K. Ekert, and A. Zeilinger, eds. 2000. *The Physics of Quantum Information*. Berlin: Springer-Verlag.

Haroche, S. 1998. Entanglement, Decoherence and the Quantum/Classical Boundary. *Phys. Today* **51** (7): 36.

James, D. F. V., P. G. Kwiat, W. J. Munro, and A. G. White. 2001. Measurement of Qubits. *Phys. Rev. A* **64**: 052312.

Mandel, L. and E. Wolf. 1995. *Optical Coherence and Quantum Optics*. Cambridge: Cambridge University Press.

Naik, D. S., C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol. 2000. *Phys. Rev. Lett.* **84**: 4733.

Nielson, M. A., and I. L. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.

Schrödinger, E. 1935. Discussion of Probability Relations Separated Systems. *Proc. Cambridge Philos. Soc.* **31**: 555.

White, A. G., D. F. V. James, P. H. Eberhard, and P. G. Kwiat. 1999. Nonmaximally Entangled States: Production, Characterization, and Utilization. *Phys. Rev. Lett.* **83** (16): 3103.

Zeilinger, A. 2000. Quantum Teleportation. *Sci. Am.* **282** (4): 50.

Daniel F. V. James was born in rainy Manchester, in northwest England, within sight of the Old Trafford (home of Manchester United, the most successful sports team in recorded human history). He was educated at New College, University of Oxford, England, and at the Institute of Optics, University of Rochester, New York, where he earned his Ph.D. in optics in 1992. He came to Los Alamos National Laboratory as a postdoctoral fellow in 1994. Three years later, he became a staff member in the Atomic and Optical Theory Group at Los Alamos. Daniel specializes in theoretical optical physics, including coherence theory, diffraction, scattering, statistical optics, and quantum technologies.

Paul G. Kwiat comes from Ohio (not a place noted for good sports teams). He was educated at the Massachusetts Institute of Technology and the University of California at Berkeley, where he received his Ph.D. in physics. In 1995, after having completed a Lise Meitner postdoctoral fellowship at the University of Innsbruck, in Austria, Paul came to Los Alamos National Laboratory as an Oppenheimer Fellow and became a staff member in 1998. In January 2001, he became the John Bardeen Professor of Physics and Electrical Engineering at the University of Illinois at Urbana-Champaign. He specializes in experimental quantum optics, with an eye toward shedding light on quantum information protocols.