The Age of Entanglement

David D Nolte, Purdue University

Available at: http://works.bepress.com/ddnolte/8/
Chapter 9

The Age of Entanglement
Teleportation and Cryptography

"... because nature isn't classical, dammit ..."

Richard Feynman, 1981 [135.5]

Quantum mechanics is a venerable field of study. The year 2000 marked the 100th anniversary of the original quantum hypothesis proposed by Max Planck in November of 1900. Few current fields in physics or engineering are as old as quantum mechanics. It predates relativity, both special and general. It predates nuclear and particle physics. Quantum mechanics even predates universal acceptance of the molecular hypothesis, that is, that all matter is made up of individual molecules in thermal motion. It may be hard to believe, but this happened only after Einstein's paper on Brownian motion was published in his miracle year 1905.

Quantum mechanics was a topic of study long before the beginnings of modern solid state physics, and indeed quantum theory formed the basis of the modern theory of solids. All of modern electronics, with its semiconductor chips and computers, is a younger field of study than quantum mechanics. At the time of Planck's announcement, no-one knew that the Milky Way was a galaxy of stars. Nor did anyone realize that the so-called nebulae were other galaxies in a vast Universe of galaxies. The discovery of the expanding universe by Edward Hubble happened decades after Planck's announcement in Berlin, and evidence for the Big Bang came only several decades after that. All-in-all, most of the fields of physics that hold our attention today are upstarts in comparison to quantum mechanics.

If quantum mechanics is so old and mature, why is it the focus of so much attention? When we read late-breaking science news in popular magazines, quantum devices are in the headlines, including the recent fervor about quantum communication and computation. For such an old field of study, one for which all theoretical aspects have long ago been verified experimentally, why does it hold onto popular imagination so strongly?

The answer is not that quantum mechanics is unintuitive. Ask any college freshman who is taking introductory physics whether they think physics is intuitive, and they will fill your ears with exasperation and frustration at the seemingly unintuitive subject. Even seasoned physicists are often stumped and surprised by ordinary physics. Systems as well-understood as electromagnetics or old-fashioned mechanics can be unintuitive. Spinning tops or collections of magnets can raise hour-long debates among highly educated and savvy physicists.

In the Physics Department at Purdue University, I can usually be found in the morning between 9:30 and 10:00 attending Professor Ramdas' Coffee Club in the Solid State Library down the hall from my office. This is a loose group of nuclear, high-energy, and solid-state physicists. We have both theorists and experimentalists among our members. One of the coffee club members, Marty Becker, is an Emeritus who travels around Indiana giving physics shows to school children. He is always coming to coffee with bars and rods, balls and magnets, pails of water, or whatever, all parts of demonstrations he is developing for his show. Without fail, his demonstrations — all of them fundamental in nature and certainly classical — raise energetic arguments among the attendees. It is not unusual for there to be as many conflicting explanations of the phenomena as there are people in the room. Classical physics, is largely unintuitive to us all. Quantum mechanics, in this sense, is just as unintuitive. Therefore, it isn't that quantum behavior is unintuitive. It is that it is so utterly implausible.

The physical behavior of extremely light-weight particles, like electrons and protons, defies Aristotelian logic. The logical problems of quantum mechanics are not even that deep. They run into trouble right at the beginning of Philosophy 101 with an apparently obvious tautology: an electron is either...
a particle, or it is not a particle. This sentence is clearly true. But in quantum mechanics I can also make the following true statement: an electron is a particle, and it is not a particle. This sentence is a contradiction in classical logic (violating the proposition \(\neg(p \rightarrow \neg p)\) in the notation of Russell and Whitehead), but it strikes at the fundamental core of quantum behavior.

For indeed, an electron is a particle, and it is not a particle. It is a wave, and it is not a wave. It is found precisely where you observe it to be, yet it is nowhere before you observe it. You can know its momentum to infinite accuracy, yet only at the price of not knowing where it is. You can equally well pin it down precisely inside an atom, yet its momentum can take almost any value at all.... Every statement seems to be either a contradiction, or a restriction. This is quantum mechanics! It is not the fact that quantum mechanics is unintuitive that gives it its allure, but that it lives in states that cannot logically exist.

But they do exist. It is an unassailable fact that every prediction of quantum theory has been experimentally verified, to date. There are no stones unturned. Every system, from solids to liquids to gases to plasmas to high-energy particles, bear out every aspect of quantum theory. Quantum mechanics is one of the most thoroughly tested theories in physics, and it has passed every test flawlessly. Therefore, its logical implausibility, though a nuisance to philosophers, causes no trouble for the practicing physicist. We take the laws of quantum theory, derive their consequences, and look for those consequences in the laboratory.

Therefore, we say without fear of contradiction that quantum measurements performed on particles on our side of the Universe instantaneously affect the outcome of experiments performed on particles on the other side of the Universe. Unbelievable! We further assert that a quantum computer can simultaneously compute the answer to a million questions all at the same time, by performing only a single computation. Audacious! Let’s see how it is done.

**INTERFERING PHOTONS**

It is always best to start with those things with which we are most familiar. Therefore, before describing the quantum behavior of light, I begin with the interference of coherent light which has been discussed in several applications in the preceding chapters. We will see that much of what we understand about classical light (light made up of electromagnetic waves) can be used with only slight modification when we begin to talk about the quantum of light — the photon. For instance, we saw that interference of light inside nonlinear interferometers will allow light to control light in the all-optical Internet. And interference inside holographic crystals is the origin of imaging computers that use the full parallelism of visual images. Interference in these examples occurs because waves satisfy the principle of linear superposition, which states that any wave can be described as a sum of individual waves. For light, the electric fields of individual waves add together to produce a resultant wave that experiences constructive or destructive interference. The interference of light waves is our point of departure as we begin our discussion of quantum optical machines.

Long before Dennis Gabor thought of holography, the ingenious Thomas Young devised a simple and elegant experiment that demonstrated the wave nature of light. Young (1779-1823) was an English physician and physicist who, in his spare time, helped decipher the Rosetta Stone and demonstrate once and for all that Egyptian Hieroglyphics were phonographic in nature, shattering the romantic notion that the magic symbols could be an instance of Leibniz's universal "character". As a physician, his principal interest was in the physics of visual perception. He was the first to measure the change in curvature of the eye as it focused at different distances, and he discovered the cause of astigmatism. The three-color theory of color perception — that only the colors of red, green and blue are needed to perceive all the colors of the rainbow, used as the basis for every color computer screen today — was also one of Young's significant accomplishments.

It was through his interest in the perception of light that he came to study the effects of light passing through tiny holes in opaque screens. When he passed light through two such holes and allowed the light transmitted from each to overlap on a distant screen, he observed bands of light alternating with bands of darkness. This was an astounding discovery that defied perceived common sense at the time: that light added to light could produce darkness. Yet this is precisely the interference effect that I employed to describe holography in the last chapter. Young was able to explain the effect as a consequence of the wave nature of light. He went on to explain the colors of soap films based on this theory, as well as to explain polarization of light waves. Despite his genius, he was disparaged by the professional English physicists of
his time, principally because Isaac Newton had proposed that light was composed of particles. In England, to disagree with Newton was sacrilege and heretical. On the other hand, the continental physicists were not so loathe to debunk Newton, and Young's work gained wider acceptance after work by the French physicist Augustin-Jean Fresnel (1788 - 1827) confirmed Young's hypothesis.

An idealized experimental arrangement of Young's double pinhole experiment has a single pinhole that emits light of a pure color and illuminates two pinholes situated a small distance apart in an opaque screen. The light emitted from each pinhole illuminates a distant viewing screen, and the field of illumination of each hole overlaps with the other. On the observing screen, bands of light alternate with bands of darkness, demonstrating the coherent interference of the light coming from both pinholes. A bright band on the screen is obtained when the difference in the distances from the two holes allows the waves to add constructively. Conversely, a dark band on the screen is obtained when the difference in the distances from the two holes allows the wave amplitudes from each pinhole to subtract to produce destructive interference. If either pinhole is blocked by an opaque obstruction, the interference pattern disappears and is replaced by an even illumination from the unobstructed pinhole.

Up to this point, the discussion has been purely classical. But now we do a simple experiment to take us out of the classical regime and into the quantum realm. We reduce the intensity of the source so that it becomes extremely weak — much weaker than even moonlight. At this stage we need to relate the intensity of light to the flux of photons. A light beam is a stream of individual photons, like drops of rain in a shower, in units of photons per second per area. In the pinhole experiment we can reduce the intensity of the source so low that there can only be a single photon in flight at a time between the source and the observation screen. We replace the screen with a photosensitive plate that records the arrival of photons, allowing the photon hits to accumulate over time on the plate. This plate is something analogous to the photodetector used in your digital camera.

When we turn on the experiment, the photo-plate responds at the positions hit by a photon. After only several photons have been detected, the photo-plate may look like a set of random spots. No discernible pattern of bright and dark bands can be seen. As we continue the experiment, the spots start to clump, and now there are the beginnings of a pattern, but it is still rough. However, after continuing for a longer time, the photo-plate has bands of bright and dark and begins to look like the expected bright and dark fringes that we see in the classical experiment.

This new version of the experiment is fully in the quantum domain. The light travels as photons and arrives at the photo-plate as photons. The photo-plate responds at specific positions that are hit by single photons. There is no room in this description for classical electromagnetic waves, nor even of the interference of electric fields. The absence of classical interference is made clear by the conditions of the experiment that allow only a single photon to be in flight between the source and the screen at a time. Since only one photon is present, its electric field neither adds constructively to, nor subtracts destructively from, the electric field of any other photon. Yet the interference pattern slowly develops on the photo-plate, just as in the classical interference experiment. Where does this interference pattern come from if the photons cannot interfere with each other?

The quantum answer is that the photon interferes with itself: an answer that warrants considerable discussion. Though the photon has an electric field associated with it, we cannot view the quantum experiment as an interference of the electric field of the photon with its own electric field. Instead, something else must be interfering to generate the interference pattern that we see accumulating on the photo-plate. To understand what is interfering, we need first to understand something of quantum wave mechanics.

**Wave Mechanics**

Wave mechanics for quantum systems was developed in 1927 by Erwin Schrödinger (at age 40). Schrödinger was able to show that the behavior of quantum particles could be understood as special functions, called wavefunctions, that obeyed a straightforward wave equation that came to bear his name. The result of this theory was an understanding that, in the quantum world, particles behave like packets of waves. This is the famous wave-particle duality that has so perplexed quantum philosophers — how best to understand objects that are both particles and waves at the same time.

The meaning of the wavefunction of an elementary particle, like an electron, was not initially obvious. That interpretation was supplied by Max Born, a German theoretical physicist at the University of
Göttingen. He suggested that the squared amplitude of a quantum wavefunction at a place and an instant in time is proportional to the probability for finding an electron at that place and time. This interpretation was radical — equally as radical as the original quantum hypothesis. Whereas the wavefunction of an electron could be accurately and uniquely specified, the electron's location could only be predicted with a probability governed by the amplitude of the wavefunction.

If you take a hundred atoms, all in exactly the same quantum state (that is, the electrons of each atom are all described by the same wavefunction), and measure the positions of the electrons in each of them, you will get a hundred different answers. But if you continue preparing more atoms in identical states and measure those, you will slowly build up a distribution of electron positions that tend to cluster close to the nucleus of the atom. With enough measurements on enough atoms, you would eventually have a smooth distribution of electron positions that exactly matched the squared amplitude of the electron wavefunction for that quantum state. The important feature of this description is the difference between where the electron is before the measurement, and where the electron was found during a single measurement.

The wavefunction for an electron is a well-defined smooth function of position. At any radius away from the atom nucleus there is some value for the wavefunction. We therefore say that an electron occupies this wavefunction, meaning that the electron is simultaneously everywhere where the wavefunction has some non-zero value. In this sense, an electron surrounds the nucleus all the time. But in the act of measurement, let us say a measurement of the position of an electron using a microscopic probe of some kind, a single electron must be found at only a single location.

Photon wavefunctions behave in the same way. When Young's apparatus contains only a single photon, that photon is governed by a single wavefunction. The wavefunction fills all the space inside the apparatus, just like the electron wavefunction filled all space around the nucleus of the atom. Part of the wavefunction passes through one pinhole, and part of the same wavefunction passes through the other. When these parts of the wavefunction overlap on the screen, the amplitudes of the wavefunction add and subtract in just the way that the electric fields of classical light waves would. When the path length differences make the crests and troughs of the wave functions line up, constructive interference occurs, and the squared amplitude of the quantum wavefunction is a maximum. Using Born's interpretation, this means that there is a high probability to detect the photon at this location. On the other hand, in regions of destructive interference, the squared amplitude of the photon wavefunction vanishes, as does any chance to observe the photon at that position.

You will note that the quantum theory gives the same answer as the classical theory. It looks like a sleight of hand to say that a photon is governed by an interfering probability wave, while at the same time the classical interference of the light fields produces exactly the same intensity pattern. This starts to look like a metaphysical question. If the quantum theory predicts an outcome that is identical to classical theory, do we really care? And more importantly, can the quantum theory predict any behavior that is impossible classically? The answer is yes — in volumes! The entire field of quantum information rests on specific differences between classical and quantum behavior. To illustrate the unnatural quantum behavior of photons I turn to a process known as "quantum seeing in the dark."

**Quantum Seeing in the Dark**

In your mind's eye, envision a diabolical terrorist who places Young's apparatus in a crowded theater. Inside the apparatus there may be (or may not be) a bomb that will detonate any time it is hit by a photon. If the bomb is there, it is placed behind one of the pinholes. As a member of the Quantum Bomb Squad, you are called in to determine whether the apparatus contains the bomb or not. Your goal is to detect the presence of the bomb without detonating it. However, all you can use to detect the bomb is a source of photons. How would you use photons to detect a photo-sensitive bomb without detonating it? If you shine photons (let's say by opening the apparatus) on the bomb to see if it is there, then it will go off and you lose your job (if not your life). But if you were a good quantum student in school and have full faith in the Born interpretation of the quantum wavefunction, you devise a way of using quantum interference to detect the bomb without detonating it, at least with odds you are willing to live with. This is what you do.

You take the apparatus, turn on the photo-plate, and then hold your breath as you send in a single photon from the source. The single photon can pass either through the open hole, or through the hole with the bomb behind it. It will do either with a 50 percent probability. If it passes through the hole with the
bomb, then it detonates, destroying valuable property, and you lose your job on the Quantum Bomb Squad. On the other hand, if it passes through the open hole, it will register a flash on the photo-plate. This is where your understanding of quantum mechanics is crucial.

If the photon hits a location on the photo-plate that would be inaccessible when both pinholes were clear, that is, a position of destructive interference caused by the wavefunction interference from the two pinholes, then the bomb must be present and you should evacuate the theater. In this result, you have detected the bomb with a photon, yet the bomb detected no photon because it passed through the open pinhole. How does the photon detect the bomb without detonating it, or even touching it? The answer is that the photon wavefunction extends throughout the apparatus. If the bomb is blocking the pinhole, it also blocks the photon wavefunction and prevents interference at the photo-plate. Therefore, blocking the wavefunction is not the same as blocking the photon itself. The wavefunction just determines where the photon is likely to go.

Unfortunately, the odds are not great that the photon will hit exactly at a location of complete destructive interference. It is more likely that the result will be ambiguous (by hitting in a location that would be accessible whether the pinhole is blocked or not). Then you will need to send in another photon, with another 50 percent chance of detonation. And if that result is ambiguous, you need to send in yet another photon, until you are most surely going to need to find a new job. Fortunately for you, there are higher-probability ways of detecting bombs in the dark.

One way is to replace Young's apparatus with a simple interferometer composed of a half-silvered beamsplitter, two mirrors, and a photodetector. This configuration uses the beamsplitter to split the possible photon paths. When photons hit the beamsplitter, they either continue traveling to the right, or are deflected upwards. After reflecting off the mirrors, the photons again encounter the beamsplitter, where, in each case, they continue undeflected or are reflected. The result is that two paths combine at the beamsplitter to travel to the detector, while two other paths combine to travel back along the direction of the incident beam.

The paths of the light beams can be adjusted so that the beams combining to travel to the detector experience perfect destructive interference. In this situation, the detector never detects light, and all the light returns back along the direction of the incident beam. Quantum mechanically, when only a single photon is present in the interferometer at a time, we would say that the quantum wavefunction of the photon interferes destructively along the path to the detector, and constructively along the path opposite to the incident beam. It is clear that the unobstructed path of both beams results in the detector making no detections.

Now place the light sensitive bomb in the upper path. Because this path is no longer available to the photon wavefunction, the destructive interference of the wavefunction along the detector path is removed. Now when a single photon is sent into the interferometer, three possible things can happen. One, the photon is reflected by the beamsplitter and detonates the bomb. Two, the photon is transmitted by the beamsplitter, reflects off the right mirror, and is transmitted again by the beamsplitter to travel back down the incident path without being detected by the detector. Three, the photon is transmitted by the beamsplitter, reflects off the right mirror, and is reflected off the beamsplitter to be detected by the detector.

In this third case, the photon is detected AND the bomb does NOT go off, which succeeds at "quantum seeing in the dark." The odds, now, are much better than for Young's experiment. If the bomb is present, it will detonate a maximum of 50 percent of the time. The other 50 percent, you will either detect a photon (signifying the presence of the bomb), or else you will not detect a photon (giving an ambiguous answer and requiring you to perform the experiment again). When you perform the experiment again, you again have a 50 percent chance of detonating the bomb, and a 25 percent chance of detecting it without it detonating, but again a 25 percent chance of not detecting it, and so forth. You keep sending in photons until you have either detonated the bomb, or detected it. Your chances of success in the end are one in three. These are much better odds than for the Young's apparatus where only exact detection of the photon at a forbidden location would signify the presence of the bomb [136].

It is possible to increase your odds even above one chance in three. You do this by decreasing the reflectivity of the beamsplitter. In practice, this is easy to do simply by depositing less and less silver on the surface of the glass plate. When the reflectivity gets very low, let us say at the level of 1 percent, then most of the time the photon just travels back along the direction it came and you have an ambiguous result. On the other hand, when the photon does not return, there is an equal probability of detonation as detection. This means that, though you may send in many photons, your odds for eventually seeing the bomb without detonating it are nearly 50 percent.
These are about the best odds you are going to get [137], but this is impressive in itself. To be able to "see" something without ever having the photon "touch" it is only possible in a quantum world. This serves to illustrate how one must reason when dealing with quantum systems, and it gets us in the habit of thinking about photons and beamsplitters, which will be useful when we begin our discussion of entangled photons. But before we talk about that, we need to understand a physical property of photons called photon polarization, because quantum information can be stored in the two orthogonal polarizations of light.

**PHOTON POLARIZATION**

One of Thomas Young's innumerable contributions to physics was the idea of polarization. He correctly understood that the electric field of light has an orientation perpendicular to the direction the light is propagating. When the electric field points in a constant direction, say in the vertical direction, or along a $45^\circ$ diagonal, we say that the light has linear polarization.

In a plane, there are always two mutually orthogonal (right-angle) directions, like the x and y axes pointing in the horizontal and vertical directions. Any linearly polarized wave can be expressed as the sum of two polarizations that point along these two mutually orthogonal axes. What you call "vertical" or "horizontal" is actually your choice. For instance, you could call a line making a $+45^\circ$ angle the "vertical" axis relative to a line making a $-45^\circ$ angle that you would call "horizontal". The choice of a direction changes only how you describe the wave's polarization — it cannot change the actual physical state of the wave. This is an important feature of all physics. It is a form of relativity. Your choice of a coordinate frame, even the frames orientation, cannot alter the physics. We are free to choose and define any axis as "vertical", and the orthogonal axis as "horizontal". Any choice is arbitrary, yet equally valid as a way of describing the electric field or the wave.

When we stop thinking of light as classical electromagnetic waves and think instead of photons, the notion of polarization remains, but the interpretation changes. A photon has a polarization just like a classical light wave, but the polarization now is associated with the photon wavefunction. If a photon is originally polarized at an angle relative to the horizontal, we say that the wavefunction is a linear combination of two wavefunctions describing two different photons, one that has a polarization along the vertical and another that has a polarization along the horizontal.

Nature has provided us with an ideal method for separating a flux of photons into the ones polarized along the vertical from the others polarized along the horizontal. This is accomplished using a crystal of calcite that has the chemical name of calcium carbonate. It is the most common constituent of limestone and marble. In its pure crystalline form it is transparent and colorless, and is noted for its property of double refraction; anything you look at through the crystal has a double image. Natural light has equal amounts of orthogonal polarizations, and the calcite crystal directs light of the two polarizations along two different directions that leave the crystal in two different locations, that we call the H and V"ports" (for horizontal and vertical polarized photons).

The calcite crystal is known as a polarization analyzer. It takes any input beam and breaks it down into its vertical and horizontal components. As an optical device we say that it has one input port, and two exit ports. Detectors are placed at both of the exit ports. If the crystal is very pure, none of the light energy is absorbed, and all of the light is detected. For a classical light wave with a polarization angled at $45^\circ$ relative to the horizontal axis, half of the intensity is detected in the V port, and half is detected in the H port because the electric field of the photon has equal parts of V and H.

Now let's consider the quantum behavior of the calcite when we send a single photon polarized at $45^\circ$. In the quantum case, the entire photon emerges whole from either one port or the other, but never both ports, and never as a fraction of a photon. For example, a photon with a polarization of $45^\circ$ is a superposition of two different photons, one with a vertical polarization and one with a horizontal polarization. The photon has 50 percent probability of exiting the V port, and a 50 percent probability of exiting the H port. If it exits from the H port, it has 100 percent H polarization. Similarly, if it exits from the V port, it has 100 percent V polarization.

When we consider the action of the calcite crystal on a single photon, we may ask an apparently simple question: Does the crystal simply observe the polarization of the photon, or does it modify it by rotating its polarization? Let us assume, for the moment, that the second option is true, that the crystal
modifies the photon. Many materials rotate the polarization of a light beam. For instance a solution of corn syrup rotates the polarization of a light beam as it propagates through the liquid by a process known as optical activity. Corn syrup is optically active because the sugar molecules, called dextrose, in the syrup have only a right-handedness. Light polarizes the dextrose molecules, and the radiated light field is rotated slightly to the right. This effect accumulates over distance into a macroscopic rotation of the polarization of the light beam.

With this in mind, we can try to explain the effect of the calcite crystal as polarization rotation. For a 45° polarized photon passing through a calcite crystal, the crystal either rotates the polarization right by 45°, or left by 45°. But this is not deterministic as it was in the case of the corn syrup. For the syrup, the rotation was always to the right. In the case of the calcite, the photon polarization for a series of identical photons is rotated right for half of them (on average) and left for the other half. On any given instance it is impossible to predict which will occur. Since the result is indeterminate, it is impossible to assign a specific physical rotation mechanism to the process. Therefore, we have no choice but to accept that calcite is not rotating the polarization, but rather is making a quantum observation, i.e., determining whether the photon has V or H polarization.

This example illustrates the fundamental indeterminacy of quantum mechanics. It is impossible to predict exactly which polarization will exit the crystal for a single incident photon. This type of indeterminacy was what Einstein was unwilling to accept. He viewed this type of experiment as evidence that quantum mechanics was incomplete. In this regard, it is important to make the distinction between “incomplete” and “incorrect”. Einstein never considered quantum mechanics to be incorrect. He was fully aware that quantum theory accurately predicted the outcomes of quantum experiments. In fact, he was the theoretician who, using quantum theory, correctly predicted many of those outcomes. Einstein's argument against quantum mechanics was rather that, in those areas where it could say nothing, as in the prediction of the result of a single observation of a single quantum particle, some deeper and more complete theory could predict the outcome. It is in this sense that Einstein considered quantum mechanics to be incomplete.

**The EPR Paradox**

It is fitting that the most imaginative and sustained attack on the completeness of quantum theory was devised by Einstein (along with Boris Podolsky and Nathan Rosen) in the EPR paradox of 1935. The paradox was introduced briefly in Chapter 2, but let's consider the paradox in more detail because it is the only way to understand quantum entanglement and quantum teleportation. To illustrate the paradox, I use a formulation along the lines proposed by the physicist and quantum philosopher David Bohm (1917-1992) that is simpler to think through. This formulation begins with the self-annihilation of an atom-like entity called positronium into two photons.

Positronium is an electron bound to its anti-matter pair, a positron, in a quantum state similar to that of a hydrogen atom. Unlike hydrogen (which is stable for times at least as long as the age of the universe), the electron and positron annihilate each other in a flash of energy that produces two gamma rays. The atom lives for only about a tenth of a microsecond, on average, before annihilation. When the positronium is initially at rest, and is in its ground state, the atom has no linear momentum and no angular momentum [138]. By the law of conservation of momentum, the final state must also have no net linear or angular momentum. We therefore immediately conclude that the two photons must travel in opposite directions, carrying equal amounts of energy and momentum, and the sum of their individual angular momenta must be zero.

Now consider a thought experiment in which many individual positronium atoms sequentially self-annihilate, and the linear polarization of the two decay-product photons are observed by two observers (we will call them Alice and Bob) who are located opposite each other and very far away from the source. (It has become a well-established tradition, in discussions of this sort, to give the name "Alice" to observer A, and the name "Bob" to observer B as a convenient device.) We insist that the difference between the observation times must be much shorter than the time it takes for photons to travel from the source to either observer. This ensures that no information about one measurement causally (that is, traveling at the speed of light) affects the outcome of the other measurement.
In Bohm's thought experiment, therefore, Alice and Bob each have a crystal of calcite with single-photon detectors placed at both the H and V output ports of their respective crystals [139]. Each chooses any angle they please from observation to observation. Neither Alice nor Bob knows what the other is doing. Each chooses a large number of angles, recording in their notebooks whether the H detector or the V detector flashed for each case. What each observer sees locally, as the experiment is progressing and as they randomly choose their measurement angle, is that whenever their H detector flashes, the V detector does not flash, and vice versa. Each photon exits the crystal in either one port or the other, but never both and never none. The observers also note that there is equal probability for the photon to appear in the H port as the V port. In other words, their local data is extremely uninteresting; they just see a long random string of photon hits in either one detector or the other with a 50/50 probability for each detection regardless of what angles they choose for their crystals. No other structure is visible in their data.

When the experiment is over, the Alice and Bob pack up their equipment and travel back to the source to compare their seemingly random data of "H"s and "V"s. To their surprise, they find that whenever they had accidentally chosen the same angles for their crystals, that they got exactly the same results. If Bob saw his V detector flash, then Alice saw her V detector flash. There were never any exceptions. One way to interpret this result is that when a polarization measurement is made on one photon, the twin photon instantly acquires the identical polarization. The effect is instantaneous, which means that no matter how far apart the two photons are when the first measurement is made, whether they are at opposite sides of an experimental optical bench in a laboratory, or are at opposite sides of the universe, as soon as the first measurement is made, the second photon instantaneously assumes the identical polarization. This "influence", being instantaneous, must therefore occur at speeds exceeding the speed of light. Such an "influence", or effect, is called "nonlocal" to contrast it with conventional forces that only exert their influence at speeds limited by the speed of light. It is precisely this nonlocal nature of the effect that Einstein and his EPR colleagues objected to, and that violated their sense of physical reality.

This paradox, to Einstein's thinking, was further evidence that quantum mechanics was incomplete. Just as he was unwilling to accept that each quantum event occurred at random, he also believed that nonlocality was unphysical. To banish nonlocality, as well as randomness, from the interpretation of quantum theory required the existence of some unknown element that determined ahead of time what polarization a photon would assume during a measurement. This unknown element is called a hidden variable.

Hidden variable theories sprang up in abundance in the early days of quantum mechanics in attempts to solve the randomness and nonlocality problems. One idea was that each quantum particle carried along with it some hidden variable that determined whether it would pass through the V port or the H port. Such a hidden variable would solve the nonlocality problem because the photon polarizations are predetermined. Each photon would already know how their twin would pass through a polarizer and therefore would require no influence traveling faster than the speed of light to tell them. It was in the context of hidden variables that he proposed his alternative EPR paradox based on measuring polarizations. His hidden variable theory was considerably more sophisticated than the one I presented. Nonetheless, we can still ask whether any of these hidden variable theories might actually be able to complete the quantum picture of reality.

This was the question asked by John Bell, an Irish physicist working at CERN in the early 1960's. He proved, using arguments about probabilities, that all hidden variable theories (if they permitted only local interactions among particles) must be false [139.5]. The proof was surprisingly simple, and produced what has come to be called the Bell Inequality. Any local hidden variable must satisfy the inequality. Quantum systems, on the other hand, violate the inequality. Devising a physical experiment that unambiguously demonstrates a violation of Bell's inequality was a challenging prospect. The definitive demonstration came in 1981 - 1982 when Alain Aspect and his research group performed a series of experiments of increasing sophistication that violated Bell's inequality with extremely high confidence. The most important aspect of these experiments, and the aspect that made them so difficult, was the need for the detection events of the two photons to be separated far enough so that no signal moving at the speed of light could travel from one side of the experiment to the other during the time of the measurements. This condition was absolutely necessary to guarantee that no local interaction (defined as an interaction limited by the speed of light) could explain the correlation between the two measurements.

The experiments by Aspect used an atomic beam of calcium atoms in excited states that radiated two photons as they fell back to their ground state. The two photons carried away polarizations in the same way as the two photons from positronium. The use of calcium instead of positronium significantly
simplified the experiments because the atomic beam produced copious numbers of visible photons that are relatively easy to analyze for polarization. The initial experiment was no more complicated than the problem of measuring individual polarizations with two analyzers. Already in this case they observed large deviations from Bell's inequality and hence firmly established the nonlocality of quantum mechanics. However, nagging suspicions of local influences persisted among the experiment's critics, leading Aspect and his team to devise an ingenious technique that allowed them to select the polarization angle after the photons were already in flight [140]. These experiments continued to agree with quantum mechanics and violate Bell's inequality. Since these experiments delayed the choice of polarization until after the photons were in flight, there was no way for the photons to have shared a local hidden variable when they were created.

These experiments unambiguously proved that all hidden variable theories that were concocted to solve the nonlocality problem are wrong. None of them will ever give results that agree with quantum theory. The inescapable conclusion is that quantum mechanics is nonlocal — the instant that one measurement is performed on one member of a pair of twin photons, the other photon's quantum state is immediately known, even if that state is on the other side of the universe. This statement is provably true, as John Bell demonstrated in 1964. Once nonlocality is accepted, the next most pressing question is whether this nonlocality can be used to communicate faster than the speed of light. We will see that the answer to this question is "no." But we will also see that twin photons are useful for quantum communication and computation, and they even provide the basis for quantum teleportation. To understand these points, we need to look closer at the quantum properties of the twins.

**ENTANGLED PHOTONS**

The photons from the positronium have a redundancy about them. Once Alice makes her measurement, Bob's measurement is redundant. If we know Alice's results, then we can say with certainty what Bob will see if he chooses the same angle for his crystal. Because of this redundancy, the quantum pair of photons are said to be "entangled" in a single quantum state. Rather than each particle having its own quantum wavefunction, both particles share a single quantum wavefunction. Performing a single measurement on a single photon already constitutes a measurement of the whole quantum wavefunction, so performing the second measurement on the second particle is not needed. If Alice sees her photon in her V port, then the vertical polarization is shared by both particles, so Bob's particle is immediately known to also have vertical polarization.

There are severe metaphysical problems that entangled pairs of particles present to philosophers. Even if the two entangled particles are separated by the diameter of the universe, they still belong to the same quantum wavefunction. In this sense, the nonlocality problem is primarily the problem with a macroscopic quantum wavefunction. It is a challenge to think of a quantum wavefunction, something that is supposed to operate at atomic and subatomic scales, extending over the size of the universe. As we saw, one viewpoint is that the common polarization shared by the two particles is indeterminate until the moment of measurement. At that moment, as one particle assumes a specific property, the entangled twin instantaneously assumes the same property. This viewpoint is known as wavefunction collapse. If the wavefunction is macroscopic, extending over long distances, the common wavefunction shared by both particles collapses at the moment of measurement, regardless of who makes their measurement first.

By taking this view, we can convince ourselves that making a measurement here and now on our side of the Universe instantly affects the state of the twin member of an entangled pair made on the other side of the Universe, regardless of any limits imposed by the speed of light. This interpretation is exactly what Einstein and his friends objected to, and exactly what hidden variable theories had attempted to dispense with. No satisfactory agreement has been reached between the pragmatists who merrily perform their experiments free from any guilt about philosophical ramifications, and the quantum philosophers who worry about the "real" meaning of entanglement.

From the pragmatic point of view, the instantaneous nature of wavefunction collapse does not provide a means of sending information faster than the speed of light. It is tempting to try to construct a quantum communication system in which Bob and Alice receive a steady stream of entangled particles from some central source. Bob chooses his crystal angles to be either 0° or 90°, with 0° corresponding to a "0" bit and 90° corresponding to a "1" bit. By making successive measurements on his particle, he
collapses the wavefunction instantaneously at Alice's location. If he sees the photon come out of his V port, then she will also see her photon come out of her V port — that is, if she has happened to choose the same crystal angle as Bob. If she chooses a different angle, the results of her measurement are only predictable statistically.

Unfortunately, even if Bob and Alice decide ahead of time to make only 0° and 90° measurements, they cannot send information back and forth instantaneously. The local measurements made by Alice and Bob look completely random. Photons emerge half of the time out the V port, and the other half of the time out of the H port. It is only when they meet to compare their results that meaning emerges from their measurements. This is not to say that no information is sent, only that the information cannot be recovered unless they meet. Alternatively, they may send auxiliary information to each other using conventional means (that travel at or below the speed of light). In fact, by sending just two additional (classical) bits of information that describe the results of their quantum measurements, it is possible to transport whole quantum states from one location to another. This is called quantum teleportation.

**Quantum Teleportation**

"Beam me up, Scotty," is an echo of pop culture that has reverberated since the Star Trek TV series first aired in the mid 60's. Captain Kirk of the Starship Enterprise is requesting Scotty, his chief engineer, to teleport him out of danger from the surface of some planet where he may have too boldly gone where no man had gone before. On the set of the TV show it was cheaper to "beam" a body to and fro with the low-budget of the original episodes than to have to film expensive landing and launch scenes of shuttle craft. But the transporter has become etched in popular culture, and remains one of the lasting icons of science fiction. The question is: What fundamental laws of physics does teleportation violate?

Maybe none, if the teleporting speed is slower than the speed of light. The aspect that makes a teleporter look so far-fetched is the scale of the task — and issues of scale are usually issues of technology rather than fundamental problems. If given enough time, clever engineers can often tackle scale as long as the fundamental physics is allowed. Sending a man to the Moon was a project of immense scale that surely must have seemed like science fiction to writers only a century ago. With many centuries ahead of us (let us hope), perhaps the scale of teleportation will be surmounted.

Nonetheless, the scale of the problem is daunting because the human body contains something around 10^{28} atoms and nuclei, and about fifteen times that many electrons. These would all need to be transported to maintain the complete being. There is furthermore the question of the quantum states of all those particles. Would it be enough to transport the physical electrons and nuclei and place them in identical locations, or would the exact quantum states of the particles need to be preserved in order to preserve the intangible essence of the human soul? This is a point that is hotly argued.

Some say that as long as all the neural synapses are identically configured, it would not matter whether the exact quantum states were reproduced. Others argue that consciousness is a fundamentally quantum phenomenon that would be destroyed if the quantum states were scrambled during the teleportation.

If the quantum states do matter, there is a fundamental hurdle that must be overcome to measure those quantum states and transmit the quantum information to the destination. Quantum measurement is a violent act because it destroys delicate quantum superpositions. It also destroys quantum information because it projects an unknown state, which is in a superposition of states, into only one of those states. The "presence" of those other states in the superposition is lost forever to that quantum particle. Quantum measurement is such a disruption of quantum information that theorists were able to prove a quantum non-cloning theorem. This theorem states that it is fundamentally impossible to clone a quantum state because the act of quantum measurement would disrupt the original [141]. This law would seem to place teleportation forever out of the reach of reality.

But there is a small loop-hole in the law that is just big enough to let teleportation wiggle through. The non-cloning law forbids the cloning of a particle without disrupting the original. But if the original is discarded, the law says nothing about the ability to recreate the original at the same or even a different location, leaving that possibility open.

Quantum teleportation is still faced with a conundrum. Quantum measurement of an isolated particle destroys quantum superpositions and hence destroys quantum information. The direct task of
measuring the quantum state of even a single particle and reconstructing that exact state is impossible, because the act of measurement only projects out one state of the many-state superposition. Therefore, even though the quantum non-cloning law would seem to allow the possibility of quantum teleportation, the process cannot be done by direct quantum measurement. Some alternate approach must be found.

That alternate was proposed in 1993 by Charles Bennett of IBM and Gilles Brassard of the Universite de Montreal with their collaborators [142]. They showed that Alice could start with the unknown quantum state that is to be teleported, and then use an entangled pair of particles as a quantum resource. She takes one of the entangled pair, and the other is sent to Bob. Alice makes a quantum measurement of a joint property belonging to both her entangled particle and her unknown quantum state. By doing this joint measurement, the other particle of the entangled pair would assume some of the quantum properties of the original unknown quantum state. Then Alice sends two bits of information through a classical channel to Bob, telling him how to rotate his entangled particle to reconstruct the original unknown state. The beauty of this approach is that the quantum state remains unknown to both Bob and Alice, even after teleportation. Therefore, if it had been in a delicate superposition of states before teleportation, it remains in that superposition after the teleportation. Also, the process of teleportation destroys the original state when the joint properties are measured with the entangled state, thereby obeying the non-cloning theorem.

The key to quantum teleportation is the ability of Alice to perform a measurement that provides Bob with enough information to recreate the original quantum state — but without having Alice actually measure the individual properties of the unknown state. This sleight of hand is performed through a process known as a Bell State Measurement, named after John Bell. This is a quantum measurement of an unorthodox kind where the joint properties of two particles are measured relative to each other, but no direct measurement of the individual properties of each particle is needed. Bob's particle collapses at the same time, but knowing this one Bell State does not tell Alice anything about the actual individual properties of the unknown state. On the other hand this information is all that Bob needs to know to perform the rotation on his entangled particle to get the original unknown quantum state.

The schematic arrangement for quantum teleportation is shown in the Teleportation figure. Particle 1 is the unknown state that is to be teleported to Bob. Alice and Bob share an entangled pair of photons; Alice has Particle 2 and Bob has Particle 3. Alice performs a Bell State Measurement on the joint properties of Particles 1 and 2, projecting her unknown quantum state of Particle 1 onto the entangled Particle 2. At the instant of the measurement, Bob's Particle 3 collapses into the same joint state as Particle 2 and 1. But Particle 3 is not yet in the exact state as Particle 1. To put Particle 3 into the state of Particle 1 Bob has to make one of four possible rotations on his particle. Which rotation to make depends on the results of Alice's Bell state measurement. Since there are four Bell states, Alice needs to send two bits of information classically to Bob (2^2 = 4). When Bob receives which Bell state Alice observed, he then knows which of the four different rotations to perform on his particle. Once he performs the rotation, his Particle 3 is identical to Particle 1 in the unknown quantum state.

After the teleportation, neither Bob nor Alice know what the unknown state is. Both the Bell State Measurement and Bob's rotation provide them with no information about the state of the particle. Yet by the laws of quantum mechanics and entangled states, Alice and Bob can be certain that the particle has been successfully teleported. Because Bob needs to know which rotation to perform, and he only gets this information from Alice through a conventional communication channel, quantum teleportation cannot occur faster than the speed of light. Even though the wavefunction collapse of Bob's particle is instantaneous with Alice's Bell State Measurement, no information is sent until Alice and Bob communicate through classical means. Quantum teleportation therefore satisfies relativity and hence causality, and it also satisfies the non-cloning theorem — hence violates no known physical laws.

The first quantum teleportation experiments was performed in 1997 in Innsbruck Austria and in Rome using nonlinear optical crystals to generate entangled pairs of photons and using simple beamsplitters and photon detectors to perform the Bell State Measurements [143, 144]. In the Innsbruck experiment, the quantum state could be teleported correctly (and verified) only one time out of four. But it was a start. The challenge facing teleportation experiments is the same challenge of the Star Trek transporter: one of scale. Teleportation has been accomplished in the laboratory using only one or a few quantum states. Pushing the number of teleported states, and the distances over which they are being teleported, is a severe challenge. Going from one (or a few) teleported states to teleporting 10^{30} quantum states of the human body may be beyond reach. The data rate for such teleportation, even if it took an
entire century to transmit all the quantum information of a single human body, would still be a data rate in excess of $10^{20}$ bits per second. Comparing this data rate to the simple classical rate of $10^{12}$ bits per second that we are struggling with today, tells us it would take about the age of the Universe to teleport a single human. Even with incredible improvements in data rates, teleportation of people does not look promising.

On the other hand, setting our sights on teleporting a human is probably not the best use of the technology. Quantum information contained in small systems of a few particles has potential that goes far beyond classical information. A small ensemble of quantum particles can be in a superposition of hundreds or thousands of quantum states all at the same time. Transporting these states using quantum teleportation therefore becomes an important resource, especially for a quantum computer. Teleportation can become the data bus that ports quantum information from the output of a quantum logic gate to a quantum memory device where the quantum information is stored until it is needed by another logical operation.

Aside from use in quantum logic gates there is a much more immediate need for quantum information transmission, especially if the information needs to be unassailably secure, free from any hint of an eavesdropper. Quantum effects guarantee absolute channel security through the simple fact that an eavesdropper must make quantum measurements to extract information, and the act of measurement fundamentally disturbs the information content. The presence of the eavesdropper can therefore be uncovered through simple measurements of the photon statistics, and the channel can be abandoned before any important information is sent.

**Quantum Cloak and Dagger**

Every time you make a purchase over the Internet with your credit card, the pertinent information is scrambled using an encryption scheme that multiplies two large prime numbers together. Multiplying large numbers is easy, but it is very difficult to factor them apart again. For instance, see how long it takes you to find the two prime factors of the number $N = 576,603,310,111$ [145]. This number takes 40 bits to describe in binary notation [146], and it takes my old computer (MacIntosh G4 with two processors) about 16 seconds to factor using a simple sequential search algorithm [147]. But the problem is that the time to factor a number increases exponentially [148]. A number with 128 bits would take my machine about nine million years. Of course, much faster computers and much more efficient algorithms are available. As we will see shortly, 429-bit keys have already been factored, although the technology that is needed to do this is hard to come by.

Therefore, forcing potential eavesdroppers to factor large products of primes is an excellent way to ensure privacy and is the basis of an encryption scheme called RSA (named after Rivest, Shamir and Adleman who invented the scheme in 1977 [149]) that is used almost universally for the transmission of electronic data. With this scheme, the person (let it be Alice) who wishes to receive a message publishes two public numbers. One is the product of two large prime numbers and the other is any number of choice. Using these public numbers, Bob constructs a message that he sends publicly back to Alice. Because the encryption key is completely public, as is the subsequent coded message, this scheme is called public key cryptography. Yet the encoded message can only be broken by someone who can succeed in factoring the large key into its prime factors.

As an example of the difficulty factoring large numbers that are the products of primes, Martin Gardner, writing for *Scientific American* [150], published the 129-digit number

$$N = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.00$$

plus an addition number $M = 9007$, and a message encrypted by the original RSA team using these numbers. A cash award of $100 dollars was promised to anyone who could crack the code. This was known as the challenge of RSA-129. A 129-digit number can be represented by 429 bits, and 512-bit encryption was (and still is) commonly being used in commercial RSA schemes.

A decade passed before the mathematical and computational tools were available to crack RSA-129, but it finally fell to a sophisticated attack mounted by researchers at the Bellcore research labs in 1994. They mustered a coordinated effort that used 1600 separate workstation platforms distributed internationally [151]. They succeeded in deciphering the message: **THE MAGIC WORDS ARE**
SQUEAMISH OSIFRAGE. Today, even 512-bit encryption is susceptible to such concentrated attack, which has raised the level of suggested security to 768-bit keys for personal security, 1024-bits for corporate security and 2048-bits for ultimate security [152]. Even with the powerful mathematical tools in use today, it would take a time larger than the age of the universe to factor the 2048-bit encryption. Yet even these numbers or greater can fail as advances are made in mathematical techniques in number theory. The fundamental problem is that the public key is always susceptible to attack.

On the other hand, quantum cryptography provides a means of sending information that is impervious to eavesdropping. What is needed is a quantum channel, for instance a fiber carrying single photons, between Alice and Bob. A third person, conventionally named Eve (a play on the word "eavesdrop"), is the suspected eavesdropper. How can quantum effects, especially quantum entanglement, be used to guarantee the security of the communications between Alice and Bob and keep Eve in the dark?

In cryptography by entanglement Bob and Alice receive entangled photon pairs from a central source. They each perform a long random sequence of polarization measurements along three different directions that they agreed upon publicly in advance. Each makes measurements that are completely random and completely independent of each other. The outcome of each measurement produces a photon in half the cases, just as in the case of the EPR experiment. Afterwards, Bob and Alice publicly send each other the polarization directions they chose for each measurement. They identify cases for which they had each used different measurement directions, and they then publicly send the results of only those measurements. If Eve is eavesdropping, then the quantum correlations will be perturbed. In that case, Bob and Alice abandon the channel. On the other hand, if the correlations are correct, then they conclude that Eve is not present. In that case they use their remaining data, obtained when they had chosen the same directions, as a random encryption key. Because of entanglement, they each have exactly the same random key. They use this to encrypt a message that they send over a completely classical channel.

This approach to quantum cryptography is virtually immune to attack. Furthermore, once Alice and Bob have their random key, it is virtually impossible for the public encrypted message to be decoded because the encoded message has perfectly random statistics based on their random measurements. There is no handle for a code-breaker to grab onto.

Practical implementation of cryptography by entanglement is the closest of all the quantum information technologies to becoming a "real" enterprise. An experiment conducted in Geneva, Switzerland in 1997 succeeded in sending entangled photons 10 km over a fiber without losing quantum correlations [153]. More recent demonstrations have succeeded in sending quantum information over conventional fibers installed for local-area networks, and also through several kilometers in air [154]. In addition, the dense part of the atmosphere near the Earth's surface is only about 10 km thick, which means that quantum communication with satellites is a clear possibility. These recent advances point to the feasibility of quantum communication and cryptography as real-world applications of quantum information. Given the growing importance of information security in a world that is progressively operating on-line, quantum cryptography is poised to become the first commercial quantum technology.

Furthermore, the potential of quantum computing is closely tied to quantum cryptography — for instance the parallel quantum information contained in superpositions of quantum states can be used to perform calculations that are intractable on any conceivable classical computer. One important problem like this is prime factorization. Quantum parallelism rises exponentially (like the problem of prime factorization) with the number of quantum states, providing an enormously parallel resource. This potential is so vast, and the threat to RSA so great, that research in quantum computing has become one of the fastest growing fields of science and technology.