Recent Developments in Quantum Optics

James D. Franson

The quantum theory of light predicts many interesting effects that may seem counterintuitive or even impossible from a classical point of view. Several effects of this kind have been investigated at the Applied Physics Laboratory, including a new kind of interferometry, the cancellation of dispersion between two distant media, and a new type of phase associated with the electromagnetic field. Some practical applications of these effects will be considered, including a fully operational system for secure communications based on the quantum mechanical uncertainty principle.

INTRODUCTION

Maxwell's equations are usually adequate for most engineering applications, since quantum mechanical effects might be expected to become important only when dealing with weak electromagnetic fields containing one or two photons. Recent work in quantum optics has led to the discovery of several new phenomena that may have practical applications, some of which will be described here. These effects rely on the quantum mechanical properties of individual photons and cannot be understood on the basis of Maxwell's equations.

It is now apparent, however, that quantum mechanics can also play an important role in high-intensity electromagnetic fields containing an arbitrarily large number of photons.[1–3] For example, some of the nonclassical results that will be described apply to the electric and magnetic fields produced in a transformer or electric motor. Future developments in quantum optics and related fields may eventually require greater reliance on a "quantum-engineering" approach to the design of practical systems.

This article will provide an overview of several recent developments in quantum optics at the Applied Physics Laboratory. No attempt will be made to provide a complete theoretical discussion of the origin of these effects. Instead, several examples will be given to illustrate some of the nonclassical properties of light and of electric and magnetic fields in general. These examples include a new kind of interferometry, the cancellation of the dispersion experienced by two distant optical pulses, and a new type of phase associated with the electromagnetic field. A fully operational system for secure communications based on the quantum mechanical uncertainty principle will also be described.

QUANTUM MEASUREMENTS

Quantum mechanics often gives very nonclassical results when two particles or systems are initially allowed to interact with each other so as to become correlated but are then separated by a large distance. A subsequent measurement of the properties of one of the particles will instantaneously change the state of the other distant particle. This process is known as the collapse or reduction of the quantum mechanical state of a system.

The collapse of the state of a system can be illustrated by considering two photons emitted from a common source in such a way that their polarizations are identical but unknown. The quantum mechanical state of this system will be denoted by $|\boldsymbol{\Psi}>$ and has the form

$$|\boldsymbol{\Psi}>=|x_1>|x_2>+|y_1>|y_2>. \qquad (1)$$

Here, $|x_1>$ and $|y_1>$ denote an x or y polarization for photon 1, and a similar notation is used for the polarization of photon 2. Each term in Eq. 1 corresponds to a probability amplitude whose square gives the probability of obtaining either the x or y polarizations. Unlike classical probabilities, all of the probability amplitudes corresponding to a given outcome must be added first and then squared to determine the total probability of an event.

It can be shown that the polarizations of the two photons are also totally correlated in any other coordinate frame, for example, the x',y' coordinate frame:

$$|\mathbf{\Psi}>=|x_1'>|x_2'>+|y_1'>|y_2'> . \tag{2}$$

Suppose that we measure the polarization of photon 1 and find that it was polarized along the x axis. Since we now know that photon 1 was not polarized in the y direction, the second term in Eq. 1 is reduced to zero and the quantum mechanical state of the system immediately becomes

$$|\mathbf{\Psi}>\rightarrow|x_1>|x_2> . \tag{3}$$

This changes the description of photon 2 as well, and we see that a measurement made on one particle can instantly change the state of a distant particle in this way.

One might suspect that such a process would violate the principles of special relativity. Einstein, Podolsky, and Rosen[4] did criticize this aspect of the quantum theory in a famous paper written in 1935. However, classical probability theory would also require a similar readjustment of the probabilities associated with photon 2 if some information is obtained about the state of photon 1, since their properties are strongly correlated. As a result, Einstein's objections to the quantum theory were generally considered to be only a matter of interpretation or philosophy for many years.

That situation changed in 1964, when John Bell[5] showed that any classical interpretation of such an experiment would require the instantaneous transfer of information from one location to another. The polarizations of the two photons must be measured along two randomly chosen axes, x and x', differing by an angle θ as shown in Fig. 1. According to quantum mechanics, the probability that both of the photons will be found to have the x or x' polarizations is proportional to $\cos^2\theta$. Bell showed that any classical theory in which the particles cannot exchange any information faster than the speed of light can at best give a linear dependence near $\theta = 0$ with a sharp angle as illustrated in Fig. 2. The random choice of measurement axes rules out the possibility that the photons were simply emitted with those particular polarizations. A large number of experiments[6] of this kind have given excellent agreement with the quantum theory predictions. (For a review, see Ref. 6.)

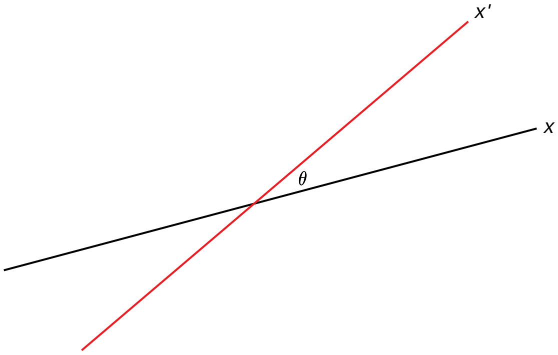


Figure 1. Measurement of the polarizations of two distant photons along two randomly chosen axes differing by an angle θ.

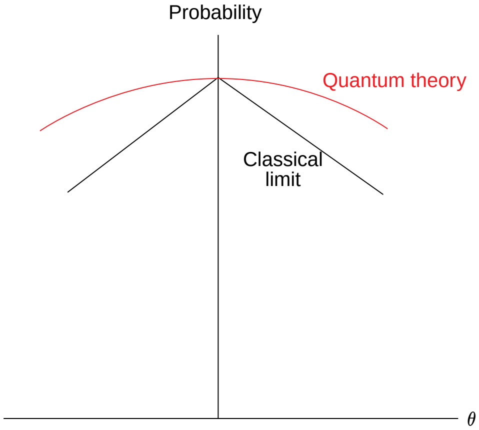


Figure 2. Probability that the measured polarizations of two photons will lie along two randomly chosen axes differing by an angle θ. The red line represents the prediction of quantum mechanics, whereas the black line corresponds to the maximum correlation in any classical theory in which information cannot be transmitted faster than the speed of light.

The fundamental difference between the classical and quantum mechanical predictions can be shown to be due to the cross products in the square of the sum of the relevant probability amplitudes. These cross products produce a nonclassical form of interference that depends on the relative phase between the various probability amplitudes.

Although a classical interpretation of these correlations would require an instantaneous transfer of information, that is not the quantum mechanical interpretation. Nor is it possible to transmit useful messages faster than the speed of light because there is no way to control or modulate the choice of polarization of photon 1, which is chosen at random at the time it is measured. Roughly speaking, photon 2 somehow receives this information instantaneously (from a classical viewpoint), but no messages can be transmitted since there can be no external control over the process.

TWO-PHOTON INTERFEROMETRY

For many years, Bell's results were only known to apply to systems with two degrees of freedom, such as the polarizations of two photons or the spins of two electrons. The author recently extended these ideas to other systems and showed that two distant interferometers can exhibit very similar correlations.[1,7–8]

To see how this situation can occur, consider a light source that creates two photons at the same time, as shown in Fig. 3. The two photons travel in opposite directions over an arbitrarily large distance, after which they encounter two identical interferometers. A beam splitter in each interferometer allows the photons to travel along a longer or a shorter path through the interferometers, and a second beam splitter allows the photons to travel toward one of two sets of detectors. The difference in the lengths of the two paths is chosen to be much larger than the coherence length of the two photons, so that no interference at all would be expected classically. As a result, each photon has a 50/50 chance of being detected in either the primed or unprimed detector.

Now suppose that photon 1 chose to propagate toward detector D_1, as indicated by an output pulse from that detector. For reasons that will be explained shortly, this information immediately reduces the state of photon 2 in such a way that photon 2 will be detected in the corresponding detector D_2 and not in D_2'. Total correlation between the chosen detectors (primed versus unprimed) is observed, provided that the sum of the interferometer phase settings is zero ($\theta_1 = -\theta_2$), whereas measurements made with other phase settings give a correlation proportional to $\cos^2[(\theta_1 + \theta_2)/2]$. Just as in Bell's original proof, the latter result is inconsistent with any classical theory in which information cannot be transmitted at velocities greater than the speed of light, since θ_1 and θ_2 can be randomly chosen after the photons have been emitted. A more detailed discussion of this experiment and related topics can be found in a recent issue of *Scientific American*.[9]

To understand how a two-photon interferometer can produce these correlations, it is necessary to consider the creation of photon pairs, which are formed by using a nonlinear crystal capable of splitting individual photons from an ultraviolet laser beam into two secondary photons, as illustrated in Fig. 4. In the quantum theory, the energy of a photon is proportional to its angular frequency ω, and its momentum is proportional to its wave vector $\mathbf{k}$, so that conservation of energy and momentum require that $\omega_1 + \omega_2 = \omega_0$ and $\mathbf{k}_1 + \mathbf{k}_2 = \mathbf{k}_0$. Here, ω_0 and $\mathbf{k}_0$ are the angular frequency and wave vector of the initial laser photons. The key feature of this process is that the two photons are created at precisely the same time, but that time is totally uncertain.[7] This situation is thus analogous to Eq. 1, where two photons have the same but unknown polarization.

The unknown time at which the pair of photons was emitted implies that a final detection event can occur in more than one way, and the corresponding probability amplitudes must be summed and then squared. A pair of photons could have reached the detectors in three ways: (1) both may have taken the longer path, (2) both may have taken the shorter path, or (3) one may have taken the shorter path while the other took the longer path. The total probability amplitude A_t for such a process can thus be written in the following form:

$$A_t = A_{ss} + e^{i[(\theta_1+\theta_2)+(\omega_1+\omega_2)\Delta T]}A_{ll} + e^{i[\theta_1+\omega_1\Delta T]}A_{ls} + e^{i[\theta_2+\omega_2\Delta T]}A_{sl} \,. \qquad (4)$$

Here, A_{ss} represents the probability amplitude that both photons took the shorter path, A_{ll} is the probability amplitude that both took the longer paths, and A_{ls} and A_{sl} are the corresponding probability amplitudes that one photon took the longer path while the other took the shorter path. A_{ll} differs from A_{ss} by a phase factor that includes the phase shifts θ_1 and θ_2 inserted into the longer paths, as well as the terms $\omega_1\Delta T$ and $\omega_2\Delta T$ due to the difference in propagation times ΔT along the longer and shorter paths.

If high-speed electronics are used to select only those events in which both photons are detected at the same time, then both photons must have taken the longer

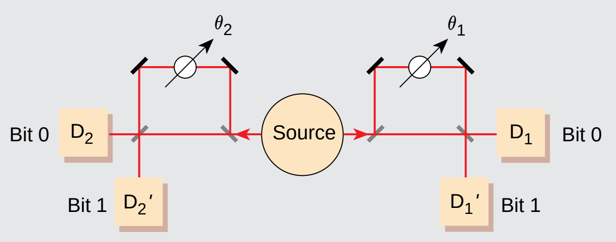


Figure 3. A two-photon interferometer exhibiting nonclassical correlations between the output ports chosen by photons γ_1 and γ_2, as indicated by single-photon detectors D_1, D_1', D_2, and D_2'. Phase shifts θ_1 and θ_2 are introduced into the longer path through each interferometer.

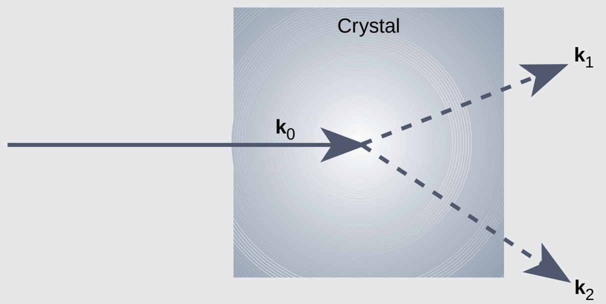


Figure 4. Individual photons from an ultraviolet laser being split into two secondary photons while conserving energy and momentum in the process.

path through the interferometers or both must have taken the shorter paths, since the two photons were emitted at the same time. The probability amplitudes A_{ls} and A_{sl} cannot contribute to the final outcome in this case and must be eliminated from Eq. 4. The total probability amplitude for coincident events then reduces to

$$A_t = A_{ss} + e^{i[(\theta_1+\theta_2)+(\omega_1+\omega_2)\Delta T]}A_{ll} \,. \qquad (5)$$

From conservation of energy, the phase factor $(\omega_1 + \omega_2)\Delta T$ is just $\omega_0\Delta T$ and produces a constant phase offset; if that were not the case, the large spread in the frequency of the two photons would destroy the interference pattern as it does classically.[8]

The total probability P_c of a coincident event is proportional to the square of the probability amplitude of Eq. 5, which can be reduced to

$$P_c = \eta \cos^2\left(\frac{\theta_1 + \theta_2}{2}\right). \qquad (6)$$

Here, η is a constant related to the detection efficiencies of the two detectors, and the constant phase factor of $\omega_0\Delta T$ has been omitted. Once again, this nonclassical result is due to interference between the probability amplitudes for the short–short and long–long processes, each of which leads to the same final outcome.

Several laboratories[1,10–12] performed two-photon experiments of this kind shortly after the publication of the author's theoretical predictions. Perhaps not surprisingly, some experts expressed considerable doubt as to the existence of such an effect. The first experimental results[10] were obtained by Ray Chiao's group at the University of California at Berkeley. Some of their data are shown in Fig. 5, which has been reproduced from Ref. 12. The roughly straight line near the top of the figure corresponds to the rate at which single photons were counted in one of the detectors as a function of the phase difference between the two interferometers; this result shows no interference due to the extremely short coherence length of the photons. However, the rate at which pairs of coincident photons were detected showed a pronounced interference pattern consistent with the theory.

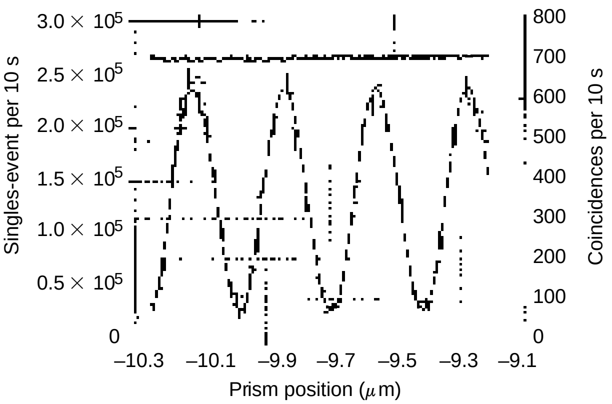


Figure 5. Results from a two-photon interferometer experiment performed by Ray Chiao's group at the University of California at Berkeley, showing interference in the two-photon coincidence counting rate but not in the single photon rates. The units correspond to the number of events of each type obtained in a 10-s interval. (Reprinted from Ref. 12 by permission.)

The author's main interest in these experiments is the question of what happens if the two interferometers are moved farther and farther apart. According to the quantum theory, the separation makes no difference. However, for some alternative theories, the interference pattern may be degraded or vanish altogether with increasing separation. An experiment was performed at APL[11] in which the two interferometers were separated by an optical path length of 100 m. Nonclassical interference effects consistent with the quantum theory predictions were also observed in that case and were independent of the separation of the interferometers. Follow-on experiments involving interferometers separated by several kilometers of optical fiber are currently in progress at APL as well as at other laboratories around the world.

NONLOCAL CANCELLATION OF DISPERSION

These nonclassical effects can be understood in more detail by considering the Fourier transform of the electric field in a beam of light. First consider the Fourier transform of a classical electric field at location $\mathbf{r}_1$, which can be expressed as

$$E(\mathbf{r}_1, t) = \sum_{k_1}\left[c_{k_1}e^{i(k_1x_1 - \omega_1 t)} + c^*_{k_1}e^{-i(k_1x_1 - \omega_1 t)}\right], \qquad (7)$$

where the $c_{k_1}$are the Fourier coefficients and t is time. (For simplicity, we are considering a plane wave and a single polarization here.) It follows from Eq. 7 that the product of the electric fields at two locations $\mathbf{r}_1$ and $\mathbf{r}_2$ is given by

$$E(\mathbf{r}_1, t)E(\mathbf{r}_2, t) = \sum_{k_1}\sum_{k_2} c_{k_1}c_{k_2}e^{i[(k_1x_1 + k_2x_2) - (\omega_1 + \omega_2)t]} + c.c., \qquad (8)$$

where $c.c.$ denotes the complex conjugate terms. It seems apparent that the product of two classical fields must contain all of the terms corresponding to each pair of Fourier coefficients in each field, as represented by $c_{k_1}c_{k_2}$.

A very different result is obtained, however, when the electric field is treated quantum mechanically.

Then the electric field becomes an operator[13,14] and the Fourier expansion of Eq. 7 is replaced by

$$\hat{E}(\mathbf{r}_1,t)=\sum_{k_1}\left[\hat{a}_{k_1}e^{i(k_1x_1-\omega_1 t)}+\hat{a}^{\dagger}_{k_1}e^{-i(k_1x_1-\omega_1 t)}\right], \tag{9}$$

where $\hat{a}_{k_1}$ and $\hat{a}^{\dagger}_{k_1}$ are operators that annihilate and create a photon, respectively. (Some constants of no interest here have been omitted.) The state of the field created by the nonlinear crystal of Fig. 4, for example, can be written as

$$|\,\Psi>=\sum_{k_1}c_{k_1}a^{\dagger}_{k_1}a^{\dagger}_{k_0-k_1}\,|\,0>. \tag{10}$$

This equation corresponds to the creation of photon pairs whose wave vectors sum to $\mathbf{k}_0$ as required by conservation of momentum. The average product of the fields at two locations can then be shown to have the form

$$<\hat{E}(\mathbf{r}_1,t)\hat{E}(\mathbf{r}_2,t)>=\sum_{k_1}c_{k_1}e^{i[(k_1x_1+k_2x_2)-(\omega_1+\omega_2)t]}+c.c., \tag{11}$$

where $k_2 = k_0 - k_1$. This result differs from the classical result of Eq. 8 in that the product of two quantum mechanical fields need not contain the cross product of every pair of Fourier coefficients that appears in the individual fields. Instead, only those coefficients whose frequencies add up to ω_0 appear in the product of the two fields. This cannot occur classically, as can be seen from Eq. 8, which explains the origin of most of the nonclassical effects of interest here. Two systems whose quantum mechanical state cannot be written as the product of the states of the individual systems are often referred to as "entangled." The polarization state of the two photons in Eq. 1 is entangled in this sense, as is the state in Eq. 10.

A further example of the kind of nonclassical effects that can result from the entanglement of quantum states is illustrated in Fig. 6. Here, two short optical pulses are propagating in opposite directions in two dispersive media, such as two optical fibers. Classically, each of the two pulses will broaden by an amount that depends only on the dispersive properties of the medium through which each is traveling; it seems obvious that the broadening of a pulse cannot depend on the properties of a distant medium through which it is not propagating.

That is not the case in quantum optics, however, where the author has shown[15] that the dispersive properties of one medium can be made to cancel out those of another medium in such a way that neither pulse is broadened. To see how this surprising result is obtained, we need to write the magnitude of the wave vector $\mathbf{k}$ in each medium as a function of the frequency ω using a Taylor series expansion:

$$\mathbf{k}_1(\omega_1)=k_{10}+\alpha_1(\omega_1-\omega_0)+\beta_1(\omega_1-\omega_0)^2+\ldots\,. \tag{12}$$

A similar expression is used for $\mathbf{k}_2$. Here, k_{10}, α_1, and β_1 are constants, and it will be assumed that the bandwidth is sufficiently small that the higher-order terms can be neglected. If we consider the case in which $\beta_2 = -\beta_1$ and substitute Eq. 12 into Eq. 11, then it can be seen that the effects of the dispersion coefficient β_1 in one medium are canceled by those of β_2 in the other medium in such a way that the dispersion has no effect on the product of the two fields and the photons remain coincident at all times. Effects of this kind are referred to as being nonlocal, since the behavior of the two pulses cannot be determined from their local environments.

This effect has also been demonstrated experimentally[16] and could conceivably be of practical use in overcoming the effects of dispersion in optical communications systems.

DYNAMIC PHASE OF THE ELECTROMAGNETIC FIELD

The phase of the electromagnetic field plays an important role in such applications as interferometry, heterodyne and homodyne detection, and communication via phase modulation. The author recently showed[2] that there is a new type of phase associated with the electromagnetic field that is totally unrelated to the classical phase normally measured. It is referred to as the dynamic phase of the field since it vanishes in the limit of slowly varying currents.

One of the general principles of quantum mechanics is that it must agree with classical physics in some suitable limiting case. The most nearly classical state of the field is referred to as a "coherent state" and can be written in the following form:[13,14]

$$|\Psi>=e^{i\gamma(t)}e^{-\alpha^2/2}\sum_{n=0}^{\infty}\frac{(\alpha e^{i\phi})^n|n>}{\sqrt{n!}}. \tag{13}$$

Here, α is a real number, ϕ is an arbitrary phase angle, and the state of the field containing exactly n photons is designated by $|\,n>$. It is well known that a beam of light produced by a laser is described by such a coherent state. The electric and magnetic fields produced by a macroscopic current distribution, such as those in a transformer or electric motor, are also described by a coherent state.[2] Thus, a quantum mechanical study of what might be thought of as classical fields would proceed starting from Eq. 13.

The classical phase of the field can be shown to be the phase factor ϕ, since the electric field operator in Eq. 9 changes the number of photons by ±1 and the corresponding states differ by a phase factor of $\pm\phi$.

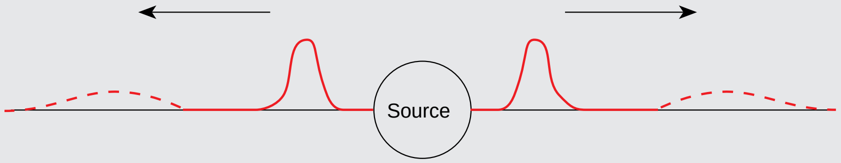


Figure 6. Dispersion of two classical optical pulses emitted by a source and propagating in two dispersive media. In quantum optics, the dispersion experienced by one photon can be canceled by that experienced by a distant photon.

However, in addition to ϕ, the author recently showed the necessity of including an additional phase factor of $e^{i\gamma}$ in Eq. 13. This new phase factor is governed by the equation

$$\frac{d\gamma}{dt} = \frac{1}{2} \frac{\int \mathbf{j} \cdot \langle \mathbf{A} \rangle d^3\mathbf{r}}{\hbar} , \qquad (14)$$

where $\mathbf{j}$ and $\mathbf{A}$ are the current density and vector potential, respectively, and $\hbar$ is Planck's constant divided by 2π.

This is a very interesting result since an electron moving in an external magnetic field undergoes a phase shift given by the same formula but without the factor of 1/2. For an electron, such a phase shift can be measured using a superconducting quantum interference device, which currently provides the most accurate method available for measuring weak magnetic fields. Equation 14 shows that the electromagnetic field has a similar phase shift associated with it, aside from the intriguing factor of 1/2. An experiment is now being planned in Germany to investigate this new kind of phase phenomenon (personal communication, F. Hasselbach, University of Tubingen, 1 Mar 1995).

One of the most interesting features of this result is that it applies to the "classical" high-intensity fields that are produced in electromagnets, solenoids, transformers, and so forth. The existence of the nonzero value of γ even in these types of situations illustrates the fact that the quantum mechanical properties of the electric and magnetic fields are not limited to weak fields containing only one or two photons, as might have been imagined. In fact, the author has recently generalized the theory of two-photon interferometry to show that similar, nonlocal correlations can occur for high-intensity fields containing arbitrarily large numbers of photons.[1]

QUANTUM CRYPTOGRAPHY

In a story entitled "The Gold Bug," Edgar Allan Poe describes an adventure involving buried treasure and a secret code. Having broken the code and found the treasure, the hero of the story states, "It may be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve." Subsequent generations of spies, traitors, and powerful computers for code breaking have amply demonstrated Poe's foresight.

Quantum cryptography[17] is a new method for secret communications whose security is guaranteed by the laws of nature. Most methods of cryptography require that a secret key or code be transported from one location to another so that it can be used to encrypt or decode subsequent messages, which creates an opportunity for the secret key to be divulged to potential enemies. This problem can be eliminated by using the two-photon interferometer of Fig. 3 to establish a secret code at two different locations without having to transmit any information in the usual sense.

To see how this can be done, suppose that detectors D_1 and D_2 are taken to represent a bit zero, and detectors D_1' and D_2' are taken to represent a bit one. If a series of photon pairs are transmitted with $\theta_1 = -\theta_2$, then the choice of output ports is totally correlated and a random but common series of zeros and ones will be generated nonlocally at each location. This series of zeros and ones can then be used as the secret key to encrypt and decode data transmitted over an open communications line in the usual way. The uncertainty principle of quantum mechanics ensures that any eavesdropper will unavoidably degrade the correlations between the photons in an observable manner, as will be discussed in more detail shortly.

Quantum cryptography based on two-photon interferometry has been investigated by the author and his colleagues as well as by Rarity, Owens, and Tapster[18] in Great Britain. We have obtained better results, however, using a similar technique[17] based on the polarizations of single photons, as illustrated in Fig. 7. If the

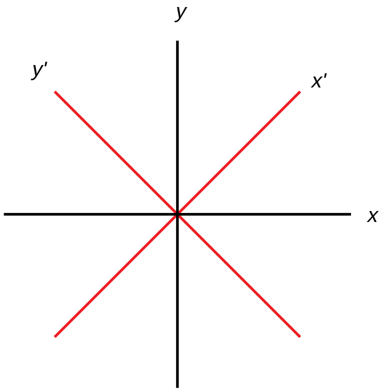


Figure 7. Two coordinate frames rotated by 45° and used for the measurement of the linear polarizations of single photons.

polarization of a single photon is measured in the x,y coordinate frame, then it will be found to be polarized along either the x or y axis; a single photon must emerge in either one or the other of the two output ports of a birefringent polarization analyzer. This is an inherently quantum mechanical effect since a measurement of the polarization of a classical beam of light can give a continuous range of values.

In our prototype system,[19–23] a secret key is generated in the following way: Two computers independently choose either the primed or unprimed coordinate frames of Fig. 7 at random. Computer 1 then transmits a single photon with a randomly chosen polarization in its coordinate frame (i.e., x, y, x', or y' polarization.) After computer 2 has measured the polarization of the photon in its coordinate frame, the two computers openly compare their choice of coordinate frames but do not disclose the polarizations transmitted or received. All events in which the computers chose different coordinate frames are simply ignored, in which case the polarizations transmitted and received will be totally correlated in the remaining events. If an x or x' polarization is taken to represent a bit 0 and a y or y' polarization is taken to represent a bit 1, then a sequence of operations of this kind will establish a common series of random bits that can be used as before to encode and decode messages transmitted over an open communications line.

The security of this approach is due to the fact that an eavesdropper does not know the correct coordinate frame and will choose the wrong one 50% of the time. If the eavesdropper simply absorbs the photon, then that event will be ignored by the two computers. The best that a potential eavesdropper can do is to emit a "substitute" photon toward computer 2 with the same polarization as he obtained from his measurement on the original photon. But if the original photon had an x polarization, for example, and the eavesdropper made his measurement in the x',y' coordinate frame, then the state of polarization of the photon will necessarily be changed. As a result, an eavesdropper unavoidably introduces an error into 25% of the polarizations as measured by computer 2, which can easily be used to detect the presence of any attempted eavesdropping. The uncertainty introduced into the polarization of a photon by a measurement made in another coordinate frame is a simple example of the uncertainty principle of quantum mechanics.

A fully operational system[22,23] for quantum cryptography is shown in Fig. 8. The main difficulty in a practical system of this kind is the fact that the transmission of a single photon through an optical fiber will produce a time-dependent change in its state of polarization due to birefringence and other factors. A feedback loop compensates for this change in polarization by varying the voltages applied to several Pockels cells, which are birefringent crystals whose retardation depends on the applied voltage. The two computers automatically determine the required voltages to transmit an x, y, x', or y' photon from computer 1 to computer 2. A third Pockels cell can be used to rotate the plane of polarization by 45°, which allows computer 2 to measure the polarization in either the x,y or x',y' coordinate frame using a fixed polarization analyzer. A photograph of the apparatus is shown in Fig. 9, and a more detailed description of the system can be found in Ref. 23.

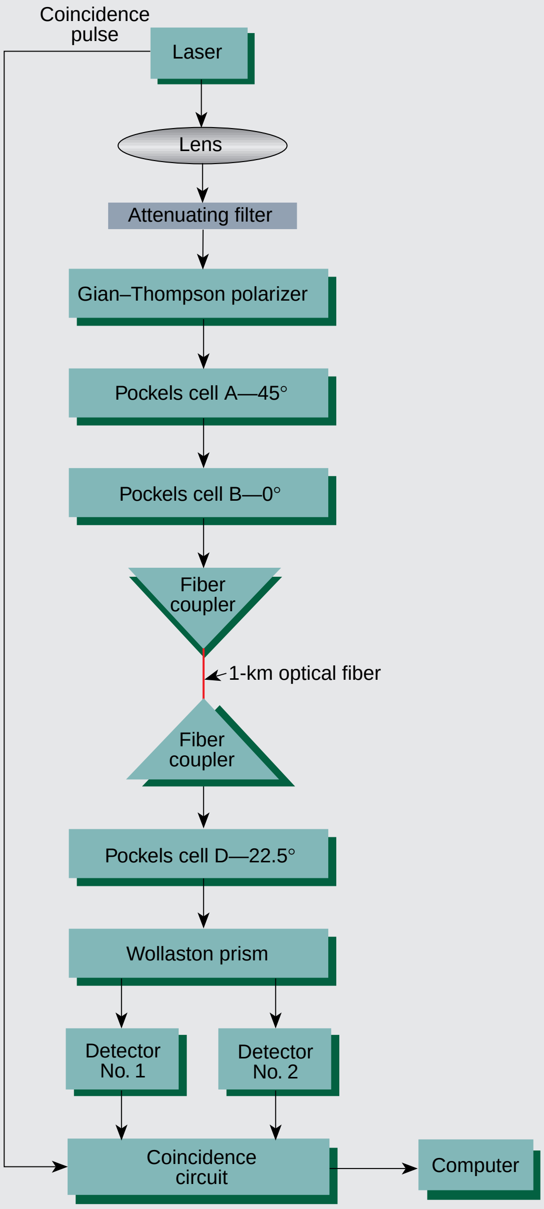


Figure 8. Block diagram of an operational system for quantum cryptography, including a feedback loop to compensate for time-dependent changes in the state of polarization of single photons propagating in an optical fiber.

This system currently allows secure communications between two personal computers at a data rate of 5 kHz. Brief messages can be transmitted from one computer to the other in a fraction of a second (Fig. 10). Higher data transmission rates will be obtained in the future using custom-made electronics to replace the logic functions currently implemented inside the computers. Any incorrect bits are identified using a secure method of parity checks; no errors have been observed in over a billion bits of secret information transmitted in this way. The system currently operates over 1 km of optical fiber; larger ranges can be obtained by operating at a more optimal wavelength. The possibility of a global system of this kind using a system of ground stations and satellites is also being investigated.

QUANTUM COMPUTING

Some of the more recent conventional cryptography systems do not require the distribution of a secret key. Known as public key systems, these methods rely on the assumed difficulty in factoring large integers. Peter Shor[24] recently showed, however, that large numbers can be factored very efficiently using a quantum computer, which may eventually compromise the security of public key systems.

Quantum computing is based on a system of quantum logic elements that have no classical counterpart. Perhaps the simplest example is the NOT function, which simply converts a TRUE input into a FALSE output, and conversely. Because quantum computing deals with probability amplitudes rather than with probabilities, it is possible to construct a logic element known as the square root of NOT. When applied twice, this logic element gives the same result as the classical NOT. But if it is applied only once, the square root of NOT produces a nonclassical operation that can be combined with other nonclassical logic elements to perform computations in a way that would be impossible classically.

Quantum computing has the potential to revolutionize computer science and is currently the subject of considerable research. Most of the investigations to date have been theoretical in nature, but several laboratories are now beginning experimental investigations as well. Quantum optics is expected to play a major role in the development of this new technology, and some of the effects described in this article are being considered for future applications of this kind.

SUMMARY

Quantum optics predicts a variety of effects that may seem counterintuitive or even impossible from a classical point of view. However implausible these phenomena may seem, the results of experiments clearly show that such effects do exist. It is hoped that further research on these topics will eventually lead to a broader range of practical applications for inherently quantum mechanical effects.

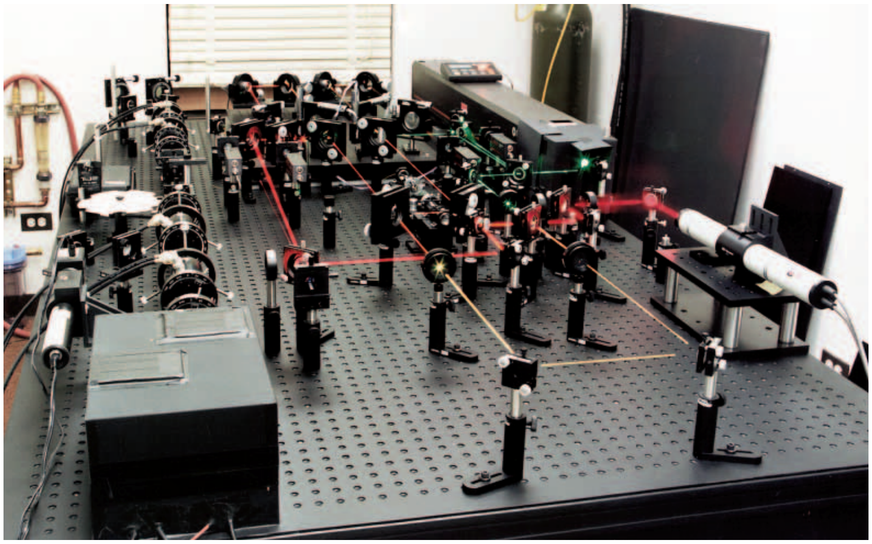
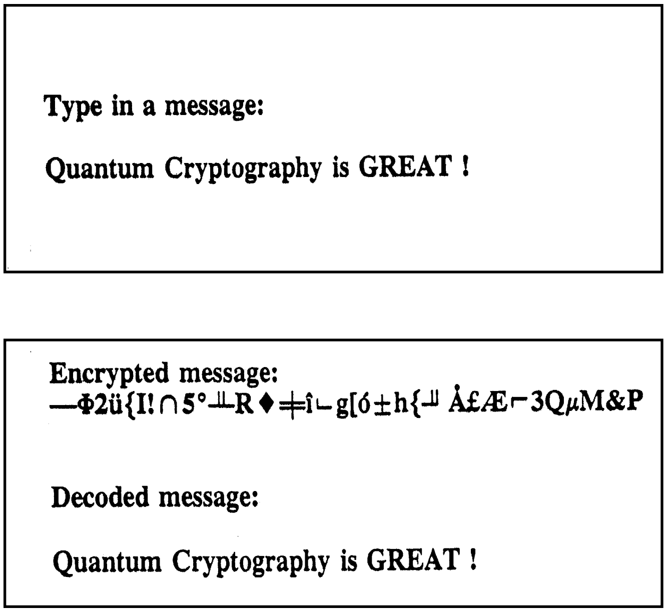


Figure 9. Photograph of the quantum cryptography laboratory at APL. The prototype system based on single-photon polarizations can be seen on the left-hand side of the optical table. The laser beams and other equipment on the right-hand side are part of a two-photon interferometer experiment.



Type in a message:

Quantum Cryptography is GREAT !

Encrypted message:
—Φ2ü{I!∩5°╨R♦╪î∟g[ó±h{╜ Å£Æ⌐3QμM&P

Decoded message:

Quantum Cryptography is GREAT !

Figure 10. Transmission of a secure message from computer 1 (top) to computer 2 (bottom). The encrypted message was transmitted over an open communications line along with the decoded message.

REFERENCES

[1] Franson, J. D., “Nonlocal Interferometry with High-Intensity Fields,” *Phys. Rev. A* **48**, 4610–4616 (1993).

[2] Franson, J. D., “Dynamic Phase of the Electromagnetic Field,” *Phys. Rev. A* **51**, 2371–2380 (1995).

[3] Munro, W. J., and Reid, M. D., “Violation of Bell’s Inequality by Macroscopic States Generated via Parametric Down-Conversion,” *Phys. Rev. A* **47**, 4412–4421 (1993).

[4] Einstein, A., Podolsky, B., and Rosen, N., “Can a Quantum Mechanical Description of Physical Reality Be Considered Complete?” *Phys. Rev.* **47**, 777–780 (1935).

[5] Bell, J. S., “On the Einstein Podolsky Rosen Paradox,” *Physics* **1**, 195–200 (1964).

[6] Shih, Y. H., and Alley, C. O., “New Type of Einstein–Podolsky–Rosen–Bohm Experiment Using Pairs of Light Quanta Produced by Optical Parametric Down Conversion,” *Phys. Rev. Lett.* **61**, 2921–2924 (1988).

[7] Franson, J. D., “Bell Inequality for Position and Time,” *Phys. Rev. Lett.* **62**, 2205–2208 (1989).

[8] Franson, J. D., “Violations of a Simple Inequality for Classical Fields,” *Phys. Rev. Lett.* **67**, 290–293 (1991).

[9] Chiao, R. Y., Kwiat, P. G., and Steinberg, A. M., “Faster Than Light?” *Sci. Am.* **269**, 52–60 (Aug 1993).

[10] Kwiat, P. G., Vareka, W. A., Hong, C. K., Nathel, H., and Chiao, R. Y., “Correlated Two-Photon Interference in a Dual-Beam Michelson Interferometer,” *Phys. Rev. A* **41**, 2910–2913 (1990).

[11] Franson, J. D., “Two-Photon Interferometry Over Large Distances,” *Phys. Rev. A* **44**, 4552–4555 (1991).

[12] Kwiat, P. G., Steinberg, A. M., and Chiao, R. Y., “High-Visibility Interference in a Bell-Inequality Experiment for Energy and Time,” *Phys. Rev. A* **47**, R2472–R2475 (1993).

[13] Meystre, P., and Sargent, M., III, *Elements of Quantum Optics*, Springer-Verlag, New York (1990).

[14] Cohen-Tannoudji, C., Dupont-Roc, J., and Grynberg, J., *Photons and Atoms: Introduction to Quantum Electrodynamics*, Wiley, New York (1989).

[15] Franson, J. D., “Nonlocal Cancellation of Dispersion,” *Phys. Rev. A* **45**, 3126–3132 (1992).

[16] Steinberg, A. M., Kwiat, P. G., and Chiao, R. Y., “Dispersion Cancellation in a Measurement of the Single-Photon Propagation Velocity in Glass,” *Phys. Rev. Lett.* **68**, 2421–2424 (1992).

[17] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., “Experimental Quantum Cryptography,” *J. Cryptol.* **5**, 3–28 (1992).

[18] Rarity, J. G., Owens, P. C. M., and Tapster, P. R., “Quantum Random-Number Generation and Key Sharing,” *J. Mod. Opt.* **41**, 2435–2444 (1994).

[19] Franson, J. D., and Ilves, H., “Experimental Comparison of Two Methods for Quantum Cryptography,” in *Proc. Quantum Electronics and Laser Science Conf., OSA Technical Digest Series,* Vol. 3, Optical Society of America, Washington, DC, p. 266 (1993).

[20] Franson, J. D., and Ilves, H., “Quantum Cryptography Using Optical Fibers,” *Appl. Opt.* **33**, 2949–2954 (1994).

[21] Franson, J. D., and Ilves, H., “Quantum Cryptography Using Polarization Feedback,” *J. Mod. Opt.* **41**, 2391–2396 (1994).

[22] Franson, J. D., and Jacobs, B. C., “Operational System for Quantum Cryptography,” *Electron. Lett.* **31**, 232–234 (1995).

[23] Franson, J. D., “Quantum Cryptography,” *Opt. Photonics News* **6,** 30–33 (1995).

[24] Shor, P. W., “Algorithms for Quantum Computation: Factoring and Discrete Logarithms,” in *Proc. 35th Annual Symp. on Foundations of Computer Science*, S. Goldwasser (ed.), IEEE Press, Washington, DC, pp. 124–134 (1994).

ACKNOWLEDGMENTS: The author would like to acknowledge the collaboration of Bryan Jacobs and Hillar Ilves in the work on quantum cryptography. Various aspects of this work were supported by the Independent Research and Development funds at APL, the Office of Naval Research, and other government agencies.

THE AUTHOR

JAMES D. FRANSON received a B.S. in physics from Purdue University in 1970 and a Ph.D. in physics from the California Institute of Technology in 1977. He joined the Strategic Systems Department at APL in 1978, where he is now a member of the Principal Professional Staff. His current research activities include quantum optics, the foundations of quantum mechanics, and atomic interferometry. His e-mail address is James.Franson@jhuapl.edu.