Quantum metrology with entangled photons

A. V. SERGIENKO

Department of Electrical & Computer Engineering and Department of Physics
Boston University - Boston, MA 02215, USA

1. – Introduction

Although most physics experiments are carried out with independent particles, it is the collective nature of entangled particles that reveals the most fascinating and unexpected aspects of the quantum world. It was Erwin Schrödinger who first said "entanglement is not one but rather the characteristic trait of quantum mechanics". One curious aspect of the behavior of a pair of particles in an entangled state is that, though each individual particle exhibits an inherent uncertainty, the joint entity of an entangled pair can exhibit no such uncertainty. As an example, while the time of arrival of an individual particle may be totally random, an entangled pair must always arrive simultaneously. This property offers a unique tool for carrying out absolute measurements. Our goal here is to explore the myriad implications and significance of entanglement and to exploit it for the development of a new type of optical measurement—quantum optical metrology.

The existence of unique non-classical correlations between twin photons generated in the nonlinear process of spontaneous parametric origins. The non-classical link between such twin quanta is not diminished by arbitrarily large separations between the twins, even when they lie outside the light cone. Twin states have been used with great effectiveness over the past two decades for carrying out definitive quantum experiments that lead to counterintuitive results; among these are those arising from the Einstein-Podolsky-Rosen (EPR) paradox such as various tests of Bell's inequalities [1-12], as well as non-local dispersion cancellation, entangled-photon–induced transparency, and entangled-photon spectroscopy with monochromatic light. The availability of these twin beams has made it possible to conduct such experiments without having to resort to

high-energy physics apparatuses such as elementary particle accelerators, colliders, and synchrotrons.

The development of the practical application and technological use of such unique quantum states was initiated about twenty years ago [13,14]. The principal objective has always been to carry out basic research at the frontier (and a bit beyond) of contemporary quantum theory, with the goal of developing useful and practical systems that outperform the limits achievable with conventional optics and imaging. Co-opting the non-local features of two-photon entangled states has allowed the opening of new vistas in the arena of high-accuracy and absolute optical measurements, which we refer to as quantum metrology. Several research projects developed over the last two decades include:

1) The design of an absolute photon source in the visible and infrared regions of the spectrum. This instrument will emit a precisely known electromagnetic-field energy with a particular wavelength, direction, and polarization. Such a device cannot be achieved within the confines of classical principles because of the presence of intrinsic fluctuations in the emission process. The non-local correlation between twin quanta permits us to conquer this limitation. Such a device would have a wide range of technological and biological applications, from measurements of the ultimate noisiness of neural circuits in the visual system to the characterization of infrared night-vision device performance.

2) A new approach to the absolute measurement of photodetector quantum efficiency that does not require the use of conventional standards of optical radiation such as blackbody radiation. This technique, too, does not exist in the realm of classical optics. The unique features of two-photon states can be traced to their origin in the vacuum fluctuations. They thus have a universal character that is everywhere present, allowing for a level of accuracy commensurate with that of a national metrology facility at every laboratory, astronomical observatory, and detector-manufacturing facility around the globe.

3) The ability to measure infrared radiation parameters without using infrared detectors and without absorption (the radiation can even be used in parallel with the measurement procedure). This technique is based on the direct use of the electromagnetic zero-point vacuum fluctuations as a global and universal reference. Infrared source temperature can be evaluated directly with the use of visible photodetectors, which have increased efficiency and reduced noise. Applications include practical uses in optical metrology, astronomy, measurements in physics, as well as in industrial and military applications including the recognition of unknown infrared signals. A principal advantage is that, again as a result of the universal nature of vacuum fluctuations, this technique does not require the use of an optical standard such as a blackbody source or synchrotron radiation. In contrast with the highly hierarchical system of national standards in current use, such a system would be viewed as the first "democratic" standard, available to any user who is cognizant of the nature of electromagnetic field and its underlying vacuum fluctuations.

4) A new approach to characterize polarization dispersion parameters of optical and photonic materials, using our ability to measure the optical delay between two orthogonally polarized signal and idler waves in SPDC with sub-femtosecond precision. We have

shown experimentally that it is possible to control the relative space-time position of two single-photon femtosecond wavepackets with attosecond resolution. This approach can be considered as quantum counterpart to conventional optical ellipsometry. The quantum entanglement of the orthogonally polarized photons in SPDC and measurement of their correlations provides us with a higher contrast, accuracy, and resolution than techniques used in conventional ellipsometry. This technique intrinsically provides an absolute value of polarization optical delay not limited by the usual value relative to one wavelength of light (2π). The single-photon intensity and the variable wavelength of our probe light do not disturb the physical conditions of the sample under test, and can be used continuously during the growth and assembly processes to monitor major optical parameters of the device *in situ*. In terms of temporal and spectral features, this approach can be considered as a single-photon alternative to the use of two well-controlled femtosecond laser pulses without femtosecond lasers.

The primary motivation for our research program is not only to develop a quantum optical material characterization technique which enhances significantly the capability of conventional ellipsometry measurement, but also to obtain detailed information about the interaction of quantum light with modern quantum microscopic semiconductor systems. This issue becomes more and more important with the increasingly significant miniaturization of modern optical devices. We expect to gain an understanding of quantum physical processes and to provide recommendations for the design and manufacturing of modern photonics systems.

5) The powerful feature of quantum entanglement between two or more quantum variables has been at the heart of a currently expanding area of research: quantum information and quantum communication. The exponentially growing flow of data transmitted every day over telecommunication channels dictates the need for its protection to insure the privacy and confidentiality of sensitive information. Conventional encryption based on the mathematical complexity of factoring large numbers is still vulnerable to the intrusion of an unfriendly party possessing a large computational power. Quantum cryptography was designed to address this issue by bringing the power of fundamental laws of quantum mechanics to protect modern communications.

We have discovered that the unique stability of a special two-photon polarization interferometer, designed to perform polarization mode dispersion measurements in optical materials, has allowed us to extend the applicability of this quantum interferometric device into the areas of quantum information and quantum communication. The area of quantum cryptography is based on the practical use of entangled two-photon state. The use of our device has allowed us to surpass the performance of cryptographic techniques using weak coherent states of light.

2. – Absolute photon source in the visible and infrared regions of the spectrum

In the course of nonlinear spontaneous parametric down-conversion (SPDC) a light from pump laser beam is converted inside a nonlinear optical crystal into sequences of
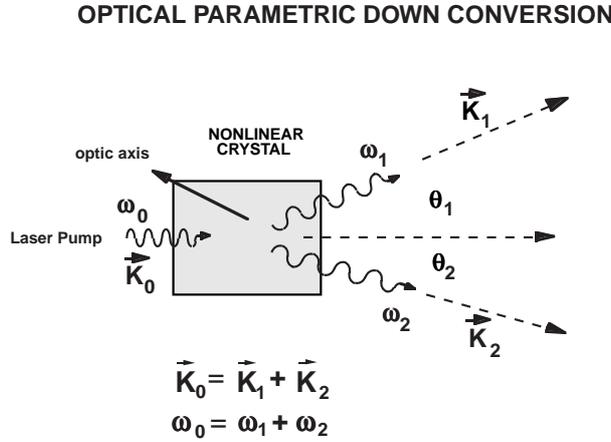
OPTICAL PARAMETRIC DOWN CONVERSION

Fig. 1. – General schematic of SPDC process.

highly correlated twin photons under the restrictions of energy and momentum conservation [15, 16]:

$$(1) \qquad \omega_1 + \omega_2 = \omega_p, \qquad \vec{k}_1 + \vec{k}_2 = \vec{k}_p,$$

where ω_p and $\vec{k}_p$ are frequencies and wave vectors (within the crystal) of the pump, and similarly ω and $\vec{k}$ refer to the down-converted output photons where $i = 1, 2$ (see fig. 1). Since the photons are created in pairs as twins, the detection of one of them indicates, with certainty, the existence of the other. Because of the energy and momentum conservation requirements, the direction and energy of the detected photon can be used to predict not only the existence, but also the direction and energy of the other photon of the pair. The process can be energy degenerate, in which case both daughter photons have the same energy; or non-degenerate, in which case the energy of the pump photon is split unequally among the two daughter photons. Thus one can be in the infrared while its twin is in the visible. This process can therefore be arranged to allow one visible photon to indicate the existence of a second IR photon, forming the basis of an extremely useful and sensitive IR measurement technique.

The majority of optical-measurement techniques record the response of that particular system when a well-known amount of optical energy is interacting with the system [17]. The main challenge is to identify the exact amount of light that impinges on a photosensitive material. The best result that classical optics can provide, for example with a laser, is an average photon number $\langle N \rangle$ with an uncertainty given by $\sqrt{N}$ as a result of Poisson statistical fluctuations. In this case, it is not possible to precisely identify the total number of photons per unit of time that impinges on the system under test. This relative uncertainty becomes substantial in case of very low intensities, which is often the case of great interest. The unique non-classical connection between twin photons in the pair allows us to solve this problem. The principle of operation is illustrated in fig. 2.
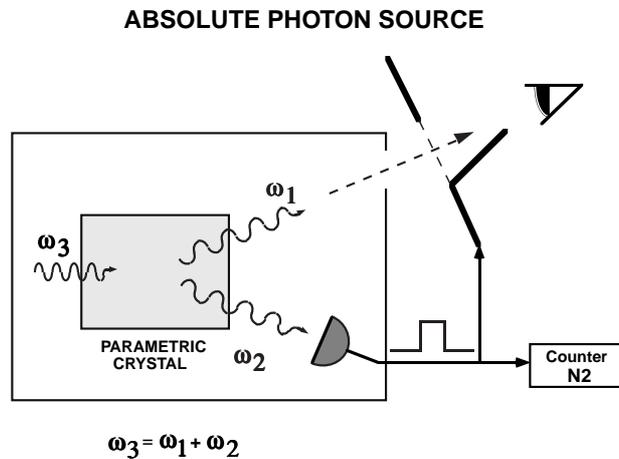
ABSOLUTE PHOTON SOURCE

$$\omega_3 = \omega_1 + \omega_2$$

Fig. 2. – Principle outline of the absolute photon source covering visible and infrared spectrum.

The photon-counting detector that registers a "green" quantum produces a voltage pulse that trumpets the arrival of its twin brother, a "red" quantum, and opens the gate for him. The electronics sees to it that the gate is closed before the next pair arrives. By counting how many times the gate has been opened, say during one microsecond, we can exactly identify the number of optical quanta (energy) of a particular color traveling in a particular direction in space. This is an absolute photon source. Such a device, which is not possible in the confines of classical optics because of the random nature of photon emissions, is expected to be very useful in a number of practical applications ranging form the accurate measurement of retinal noise in the visual system to the quality control of infrared night-vision devices that are sensitive to several photons in the infrared spectrum. A number of biological interactions that can only be carried out at very low illumination levels can also be effectively studied using such a device.

3. – Absolute calibration of quantum efficiency of photon-counting detectors

One of the important, and difficult, problems in optical measurement is the absolute calibration of optical radiation intensity and the measurement of the absolute value of quantum efficiency of photodetectors, especially when they operate at the single-photon level and in the infrared spectral range. The main objective of this proposal is to develop a novel technique for the measurement of the absolute value of quantum efficiency of single-photon detectors in the 0.4–$2\,\mu$m wavelength region of the infrared spectrum with high precision. This method can be viewed as a natural extension of the absolute photon source discussed above and cannot be achieved using classical optics. It also exploits the universal nature of the entangled super-correlation between entangled light quanta generated in the nonlinear process of spontaneous parametric down-conversion. As a result of the universal nature of vacuum fluctuations, this method does not require the

ABSOLUTE DETECTOR CALIBRATION

$$\omega_3 = \omega_1 + \omega_2$$

N_1, N_2 COUNTS RECORDED
N_C COINCIDENCE COUNTS
η_1, η_2 ABSOLUTE DETECTION EFFICIENCIES
$N_1 = \eta_1 N \quad N_2 = \eta_2 N \quad N_C = \eta_1 \eta_2 N$
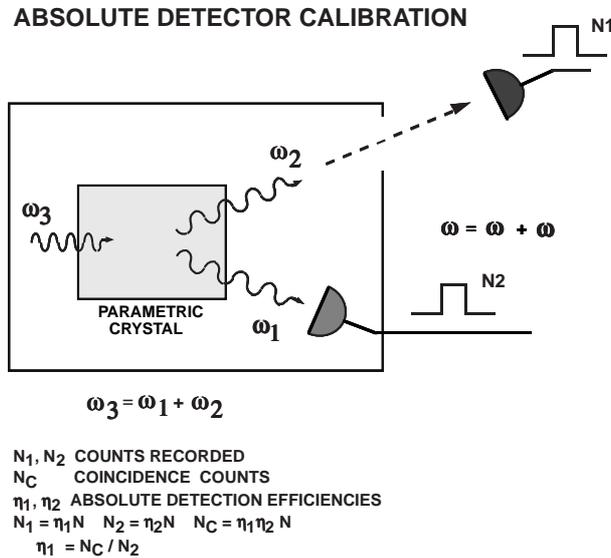$\eta_1 = N_C / N_2$

Fig. 3. – Principle of absolute calibration of quantum efficiency without using standards.

use of an external optical standard such as a blackbody radiator or synchrotron radiation source. Traditionally, two principal approaches have been used in spectroscopy, astronomy, and photometry for determining the absolute quantum efficiency: 1) comparison with an optical signal which has well-known parameters (comprising different optical standards); and 2) measurement of an optical signal by using a preliminary calibrated photoelectric detector. The physical principle used for both the optical standard and photodetector calibration methods is the spectral distribution of the intensity of thermal optical radiation, which is characterized by Planck's famous blackbody radiation law. To use this theoretical expression in practice, a number of absolute blackbody radiation sources have been constructed over the last century. Indeed, metrology institutes around the world are working on improving the accuracy of this classical measurement technique. Unfortunately, these techniques are useful only for the measurement of intense optical signals. They cannot be used for the measurement of optical radiation at ultra-low levels, nor for the determination of the quantum efficiency of single-photon detectors such as those required in astronomy and spectroscopy. It was discovered in the mid-1970s that, in theory, quantum mechanics provided a unique opportunity to develop new methods for optical measurements based on the intrinsic twin-photon entanglement inherent in light produced by spontaneous parametric down-conversion [18]. The principle of this technique is illustrated in fig. 3.

In addition to the number of pulses registered by detector 1 (N_1) and by detector 2 (N_2), we must detect the number of coincidence counts N_C. Because of the unique twin-photon character of this process all photons arrive only in pairs. The number of single photons in each arm is exactly the same as in its opposite, so that $N_1 = N_2 = N$,
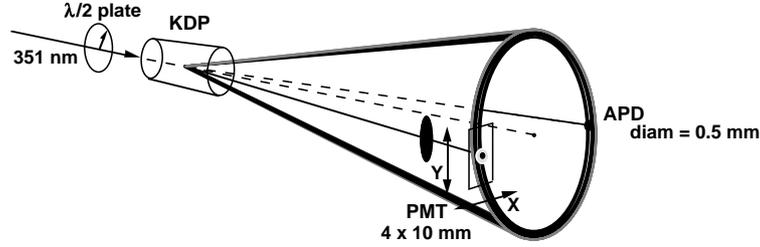
PMT SPATIAL RESPONSE MAPPING SCHEME

Fig. 4. – Outline of the experimental setup for spatial mapping of the absolute quantum efficiency.

which is exactly the number of pairs $N_{\mathrm{pairs}} = N$. As a result, the absolute value of quantum efficiency is simply determined by

$$(2) \qquad\qquad \eta_1 = \frac{N_{\mathrm{C}}}{N_2}.$$

Absolute quantum-efficiency calibration was developed further by designing a special apparatus that allows the measurement of the spatial distribution of quantum efficiency across the photosensitive area of a photon-counting device (see fig. 4) [19].

This research has included a theoretical analysis of the generation of twin-photon states for several nonlinear crystals and pump laser wavelengths in different spectral ranges, as well as the calibration of different types of detectors. A system analogous to the one displayed in fig. 4 provides us with the ability to study different types of photodetectors over a wide spectral range, including the near-infrared and infrared wavelengths. Our special efforts are directed towards developing a calibration technique for ultra-sensitive CCD cameras and towards the miniaturization of the apparatus.

4. – Calibration of quantum efficiency using single detector

In this section we demonstrate the measurement of quantum efficiency of a photon-counting photomultiplier using an entangled two-photon technique and a totally new approach that requires the use of only single photodetector. The absolute value of quantum efficiency for the photon-counting photomultiplier is derived based on the distinction between its capability of distinguishing single-photon and double-photon events. This piece of information can be evaluated by measuring the pulse-height distribution.

The photodetection process is usually characterized by the value of quantum efficiency, η, that can be used as a measure of successful conversion of optical quanta into macroscopic electric signal. If the average intensity of the photon flux (number of photons) arriving at the surface of photodetector in the unit of time is $\langle N \rangle$, then the probability of successful photodetection will be determined by $P_1 = \eta \langle N \rangle$. The probability of having no

detection event will, obviously, be defined by the complimentary value $P_0 = (1 - \eta)\langle N \rangle$. The presence of SPDC radiation consisting of rigorously correlated photon pairs with continuous distribution in a broad spectral and angular range —as a result of the non-linear parametric interaction of laser pump radiation with the nonlinear crystal— makes it possible to determine the spectral distribution of the measured quantities of photodetectors. We already know that the average number of pairs $\langle N_{\text{pairs}} \rangle$ per unit of time is equal to the number of either signal $\langle N_{\text{s}} \rangle$ or idler $\langle N_{\text{i}} \rangle$ photons:

$$\langle N_{\text{s}} \rangle = \langle N_{\text{i}} \rangle = \langle N_{\text{pairs}} \rangle. \tag{3}$$

In the case of ideal photodetector, which can perfectly separate single- and double-photon detection events by the height of the corresponding electrical pulse, this non-classical feature of SPDC light would allow us to design a simple technique for the measurement of quantum efficiency. From the theory of photodetection, the probability of having a double-photon event and a double-electron pulse will be

$$P_2 = \eta^2 \langle N_{\text{pairs}} \rangle. \tag{4}$$

The probability of observing a single-photon detection event and a single-electron pulse will apparently involve the loss of one photon in the pair. Since this can happen in two different ways for every pair, the total probability of having a single-photon detection will be

$$P_1 = 2\eta(1 - \eta)\langle N_{\text{pairs}} \rangle. \tag{5}$$

One can then conclude immediately that the value of quantum efficiency can be evaluated using the following formula:

$$\eta = (1 + P_1/2P_2) - 1. \tag{6}$$

However, the gain fluctuation and thermal noise in real photodetectors usually result in a very broad pulse-height distribution corresponding to single- and double-photon detection events. This has stimulated the development of a more realistic version of this technique that would be efficient, robust, and insensitive to such imperfections in real photon-counting detectors. In order to eliminate the influence of the broad pulse-height distribution, we can use a simple comparison between the numbers of registered detection events (regardless of their amplitude) counted in two special cases: a) when a photodetector is exposed to a pairs of entangled photons, and b) to a signal (or idler) photon only. The total probability of detecting an electrical pulse when pairs of entangled photons arrive at the photocathode will consist of the superposition of probabilities P_1 and P_2:

$$P_{\text{pair}} = P_1 + P_2 = 2\eta(1 - \eta)\langle N_{\text{pairs}} \rangle + \eta^2 \langle N_{\text{pairs}} \rangle. \tag{7}$$
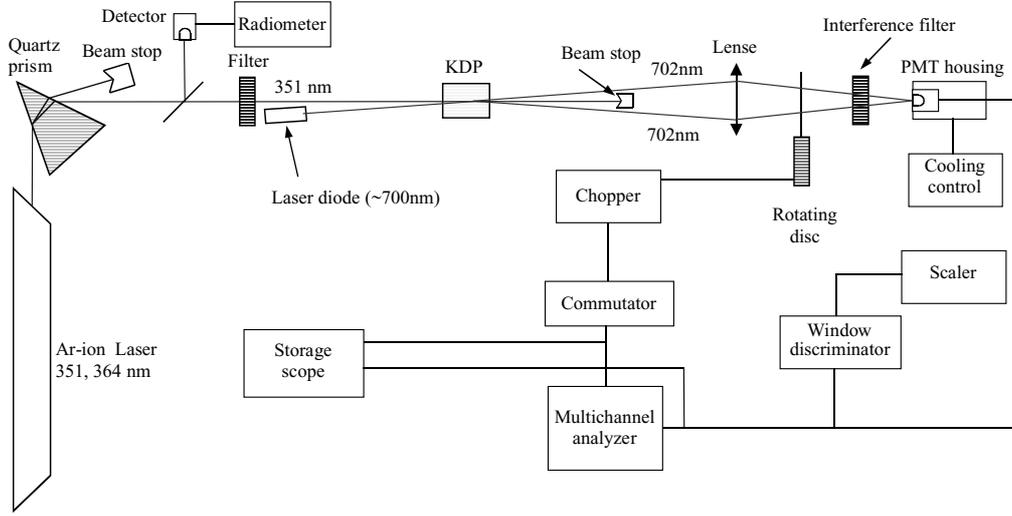
Fig. 5. – Experimental setup for the measurement of quantum efficiency using a single photodetector.

The probability of detecting a photoelectric pulse in the case of exposure to signal (or idler) photons only will be

$$(8) \qquad P_{\mathrm{single}} = \eta \langle N_{\mathrm{s}} \rangle = \eta \langle N_{\mathrm{i}} \rangle = \eta \langle N_{\mathrm{pairs}} \rangle.$$

The absolute value of quantum efficiency can be evaluated based on the results of these two measurements:

$$(9) \qquad \eta = 2 - \frac{P_{\mathrm{pair}}}{P_{\mathrm{single}}}.$$

A serious account of possible sources of thermal noise in the photodetector is required in order to enhance further the accuracy of our measurement technique. This has been accomplished by using a special measurement procedure outlined below [20].

The correlated photon pairs were generated by parametric down-conversion in KDP crystal pumped by an UV line of an argon laser at 351 nm (see fig. 5). The crystal was cut at the type-I phase matching angle (53° relative to the optical axis) to produce entangled photons of the same polarization. The non-collinear photon pairs of the same wavelength (702 nm) were selected using two diaphragms and narrow-band interference filters. To reduce the level of dark counts, the PMTs were placed in a Peltier cooling housing with temperature stabilization. The measurements were carried out at $-10\,°\mathrm{C}$. To insure separate registration of single and double photons arriving at the photocathode of PMT, we performed a special modulation of the signal and idler beams using a SR540 type Stanford Research Systems Chopper.
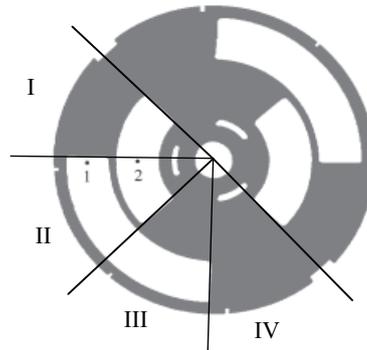
Fig. 6. – Special disk to manipulate the arrival of pairs or individual photons at the surface of the photodetector.

The rotating disk placed between the focusing lens and the interference filter in front of the photocathode has been divided into four quadrants (see fig. 6). A special synchronous commutation of memory sectors of our 16000 channel multichannel analyzer (MCA) made it possible to register in different memory sectors all contributions provided by photons from signal and idler beams separately, by the joint detection of two photons, and by the noise. The value of quantum efficiency can be evaluated using the ratio between the single- and double-photon peaks in pulse-height distribution. The amplitude distributions corresponding to the detection of single- and double-electron events using multichannel analyzer are shown in fig. 7.

The single-electron peak is well pronounced and the double electron peak is also observable. In preparation for the calculations of the quantum efficiency, we define the following terms: M_{i+b} is the total number of counts in sector I (fig. 6), $M_{i+s+si+b}$ is the total number of counts in sector II, M_{s+b} is the total number of counts in sector III, M_b is the total number of counts in sector IV (background), where i, and s, correspond to the single-photon rates of the idler and signal beam, b corresponds to the background count rate, and si corresponds to the rate of two photons detected. Statistically, in the

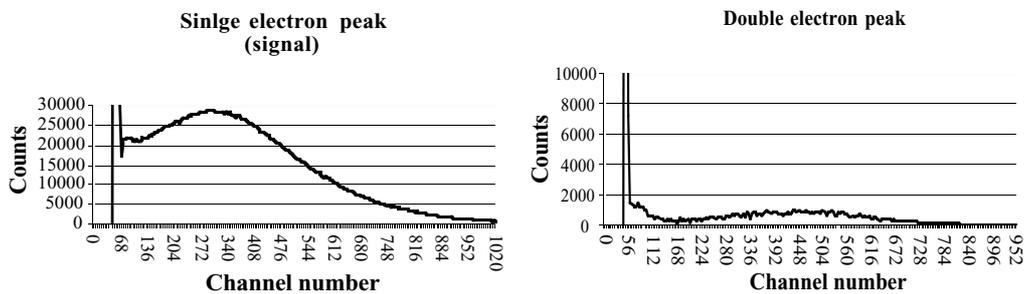Fig. 7. – Amplitude distribution corresponding to single- and double-photon peak.

case of good alignment, $M_{i+b} = M_{s+b}$. The number of single counts in sector I is

$$(10) \qquad\qquad \langle N_i \rangle \eta = \langle N_{\text{pairs}} \rangle \eta,$$

where $\langle N_{\text{pairs}} \rangle$ is the photon pairs rate and η is the quantum efficiency. The number of single-photon counts in sector II is

$$(11) \qquad\qquad 2 \langle N_{\text{pairs}} \rangle \eta (1 - \eta),$$

and the two-photon counts in the same sector is

$$(12) \qquad\qquad \langle N_{pairs} \rangle \eta^2.$$

The number of counts in sector III is consequently

$$(13) \qquad\qquad \langle N_s \rangle \eta = \langle N_{\text{pairs}} \rangle \eta.$$

In this case,

$$(14) \qquad\qquad M_{i+s+si+b} - M_b = 2 \langle N_{\text{pairs}} \rangle \eta (1 - \eta) + \langle N_{\text{pairs}} \rangle \eta^2$$

and

$$(15) \qquad\qquad M_{i+b} - M_b = \langle N_{\text{pairs}} \rangle \eta.$$

Using these two equations, the quantum efficiency value can be calculated from the following formula:

$$(16) \qquad\qquad \eta = 2 - \frac{M_{i+s+si+b} - M_b}{M_{i+b} - M_b},$$

where on the right side we find only the values which can be measured. This also prevents the thermal background noise from contributing to our result.

During one measurement cycle, the data were accumulated during 25000 periods containing four different sectors (100000 measurements), making the statistical variation of the measured distribution less than 1%. The uncertainties caused by the electronics can be due to the fluctuation of the amplitude of electrical pulses in the photomultiplier, because of the short-term and long-term instability of the high-voltage (HV) source, fluctuation of the amplification of the signal in the photomultiplier, or uncertainty caused by the electronic signal evaluation. The errors caused by the instability of HV in our measurement can be neglected because the HV is stabilized to 0.1%. This gives a much lower contribution to the pulse amplitude fluctuation than the other sources. The amplification process inside the photomultiplier gives rise to a Poissonian variation in the pulse height. The nonlinearity of the amplifier was less than 0.1%, the integral linearity of the multichannel analyzer was ±0.08%, and the differential linearity was ±0.8%.

As we calculated, the total contribution of these sources to the measurement results is less than 0.5%. The cumulative uncertainty of the reported measurement is less than 3%. For two tested type EMI 9863B/350 and EMI 9882B photomultipliers, the quantum efficiency have been measured to be 3% and 2%, respectively, at the 702 nm wavelength.

5. – Measuring infrared radiation without infrared detectors

A typical infrared experiment might be described in the following way. Radiation from the source passes first to a modulator, where either its amplitude or its phase is made to vary periodically in time. The modulated radiation then passes into the experiment area. Here it is processed in some way, interacts with the specimen under study and is registered by a detector. For the moment, one can think of the detector as an entity which produces an electrical signal whose amplitude is (hopefully) linearly proportional to the incident intensity. The signal from the detector is amplified (if necessary) up to the level required by the phase-sensitive demodulator (or PSD), the final output being an analog signal, which can either be used as it stands or else may be digitized and then processed further by a computer. The beam is modulated because a) it is much easier to process AC signals than DC ones, b) the problems of drift are largely eliminated, and c) it is much easier to suppress "noise" down to a tolerable level when using an AC system. Some sources are inherently modulated, pulsed lasers for example, but for the common blackbody sources and for continuous-wave lasers one must use an external modulator. Electro-optical modulators can be used in the near infrared, but the shortage of suitable materials makes them unavailable at longer wavelengths. In the majority of cases, therefore, the practice is to use a rotating-blade chopper. The principal exceptions occur in Fourier Transform Spectrometry (FTS), where one has available the alternative options of modulating the phase by "jittering" one of the interferometer mirrors or of achieving AC operation without explicit modulation by the use of rapid-scan techniques.

When a mechanical chopper is being used for visible or ultraviolet work, its exact location is not critical since the background is everywhere dark with only the source bright. In the infrared, however, where not only is the background glowing faintly but the specimen itself may be producing significant amounts of radiation, the positioning of the chopper is very important. To make sure that only the source is seen by the detector, the modulator has to be placed as close to the source as possible. In this way the unmodulated radiation from, say, a hot specimen will be ignored by the recording system. However, it is nevertheless still arriving at the detector. The remedy is to place the specimen as far from the detector as can be arranged so that the detector window will intercept the minimum solid angle. In mid-infrared grating spectrometers it is usual, for these reasons, to place the specimen before the monochromator. In this way one not only obtains a reduction because of the solid-angle effect, but also achieves an enormous attenuation of the specimen radiation at the slits of the monochromator and by dispersion within it. When using an interferometer these latter two benefits are not available, which incidentally is one of the disadvantages of FTS compared with grating spectroscopy.

The whole discussion of measurement leads at once to the properties of the detector,

since the rest of the equipment can be assumed to have known performance. Absolute radiometry requires a detector that is not only linear but whose output is calibrated in absolute terms. Relative radiometry requires merely that the detector be linear over its range of use. True absolute radiometers work only down to about the milliwatt level. This can be extended by the use of secondary standard radiometers, *i.e.* ones calibrated against a true primary standard, down to about the microwatt level, but it is unsafe to trust them any further. Absolute radiometers, because of their mode of construction, would be expected to be stable in time but the sensitivities of most other detectors, and especially the most sensitive ones, would be expected to be constant only over short periods.

Making a true absolute radiometer is a very difficult task because one has to compare an unknown radiant power with a known standard power under strictly equivalent conditions. Two different approaches have emerged. The first relies essentially on calorimetry, where one measures the heat rise due to the absorption of the incident radiant power. The second relies on a previous calibration of the radiometer in terms of a source of known radiant power, *e.g.* a blackbody. The first approach is sometimes thought to be more "absolute" than the second, since it goes back to measurement first principles and makes no theoretical assumptions; but in actual practice there is not much difference between the two and it is best to regard both types as equally "absolute". In the calorimetric approach, one measures the amount of heat produced when the radiation is absorbed in a thermally isolated black receiver. One could do this by having a sensitive absolute thermometer buried in the receiver and then, if one knew the thermal capacity of the receiver, one would have the magnitude of the incoming power directly. For several reasons of convenience this simple positive approach is replaced by a null technique in which the amount of electric power required to produce the same temperature rise is measured.

In the second type of absolute radiometer, IR radiation from the source with known radiation parameters and geometry (blackbody) is detected using different infrared detectors.

One of the serious potential sources of systematic error in absolute radiometry is the difficulty of getting a good match of the detector receiving geometry to the actual blackbody field distribution. This is equivalent to requiring the antenna pattern of the detector to intercept a well-known portion of the incoming energy. Another problem is that the blackbody is an ideal model: its implementations are really gray rather than truly black.

The discussion of just a few practical issues of IR spectroradiometry clearly indicates a strong need for new techniques and approaches that are based on novel principles in order to avoid old problems.

6. – Measuring the radiance of infrared light using correlated visible photons

6.1. *Brightness of vacuum fluctuations as a universal absolute reference.* – All measurement applications based on the use of non-classical optical states have two important properties: a) they are intrinsically absolute and do not rely on any externally calibrated

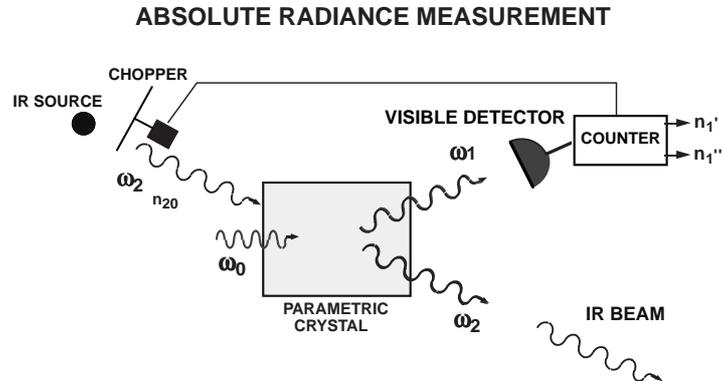**ABSOLUTE RADIANCE MEASUREMENT**

Fig. 8. – Principle of absolute spectral radiance measurement.

radiometric standards, and b) they allow for infrared radiation to be measured using visible detectors. One further characteristic of the radiance technique is that this is the only method that measures radiance directly: *i.e.*, separate radiant power and area measurements are not required.

The proposed method of measuring absolute spectral radiance without externally calibrated standards employs the process of optical parametric conversion (PC) in which individual photons from a pump beam are converted, in a nonlinear crystal, into pairs of photons.

To measure absolute radiance, a nonlinear crystal pumped by a laser is set up as just described to produce correlated IR-visible pairs of photons (see fig. 8). The output of the IR source to be measured is imaged into the crystal so as to overlap the region pumped by the laser and to overlap the output direction of a portion of the converted light.

The IR beam to be measured must overlap the converted output spectrally, as well as spatially and directionally. This additional IR input to the crystal enhances the "decay" of photons from the pump beam into converted photons along that overlap direction but, because these output photons must be produced in pairs, an increase is also seen along the correlated direction. By analogy with an atomic system, this can be thought of as a "stimulated decay" of pump photons into correlated pairs, whereas the correlated photons produced with only the pump laser for input are the result of "spontaneous decay". This "spontaneous decay" is equivalent to that produced (or stimulated) by a spectral radiance of 1 photon/mode, which can be written as $R_{\text{vac}} = hc^2/\lambda^5$ (which has the more familiar units of spectral radiance, W/m^3 sr) [18]. This value can be obtained using the following relationships:

$$(17) \qquad\qquad L(\lambda) = \frac{c}{4\pi}\, u, \qquad\quad u = \rho\, \bar{n}\, \frac{hc}{\lambda}, \qquad\quad \rho = \frac{4\pi}{\lambda^4},$$

where $L(\lambda)$ is the spectral radiance, λ is the wavelength, u is the energy density of a single polarization of a thermal field, ρ is the mode density, $\bar{n}$ is the average number of

photons per mode, c is the speed of light, and h is Planck's constant. Combining these one gets

$$(18) \qquad L(\lambda) = \frac{hc^2}{\lambda^5}\,\bar{n}.$$

From this form it is clear that a radiance of 1 photon/mode is hc^2/λ^5.

The origin of this "one photon/mode" can be understood in terms of the quantum field-theoretic description of the nonlinear parametric converter by Louisell *et al.* [21]. The three-wave interaction Hamiltonian for the optical parametric process can be written as

$$(19) \qquad H_I = \frac{1}{2}\int \mathrm{d}\nu \mathbf{P}\cdot\mathbf{E}_\mathrm{p}(r,t) = \frac{1}{2}\int \mathrm{d}\nu \chi^{(2)}_{12\mathrm{p}}\mathbf{E}_1(r,t)\mathbf{E}_2(r,t)\mathbf{E}_\mathrm{p},$$

where $\mathbf{P}$ is the nonlinear polarization induced in the medium by the pump field $\mathbf{E}_\mathrm{p}$. The polarization is defined in terms of the second-order dielectric susceptibility of the medium, $\chi^{(2)}_{12\mathrm{p}}$, which couples the pump field to the two output fields, $\mathbf{E}_1$ and $\mathbf{E}_2$. The field operators, $a_{i0}, a_{i0}^\dagger$ for the creation and annihilation of photons at the two output frequencies ω_1 and ω_2 can be written as

$$(20) \qquad a_1(t) = e^{-i\omega_1 t}(a_{10}\cosh gt + ie^{-i\varphi}a_{20}^\dagger \sinh gt),$$

$$(21) \qquad a_2(t) = e^{-i\omega_2 t}(a_{20}\cosh gt + ie^{-i\varphi}a_{10}^\dagger \sinh gt),$$

where g is a parametric amplification coefficient proportional to the second-order susceptibility, the crystal length, and the pump field amplitude; $a_{i0}, a_{i0}^\dagger$ are the initial operator values and φ is the phase determined by the pump wave phase. The average number of photons per mode in the output fields, $n_1(t)$ and $n_2(t)$, is

$$(22) \qquad n_1(t) = \langle a_1\dagger(t)a_1(t)\rangle = n_{10}\cosh^2 gt + (1+n_{20})\sinh^2 gt,$$

$$(23) \qquad n_2(t) = \langle a_2\dagger(t)a_2(t)\rangle = n_{20}\cosh^2 gt + (1+n_{10})\sinh^2 gt,$$

where n_{10} and n_{20} are the inputs into the $n_1(t)$ and $n_2(t)$ fields, respectively. Since the $\cosh^2 gt$ and $\sinh^2 gt$ factors can be considered constants (which describe the gain in a single pass through the crystal), eqs. (22), (23) can be understood as a two-component gain process with an unusual feature. The "one" in the second term causes there to be a non-zero output, even when both inputs are zero. It is this "one", that can be thought of as the one photon/mode "stimulating" the *spontaneous* conversion process. The ratio of the n_1 output with and without an input added to the channel n_2 is just

$$(24) \qquad \frac{n_1(\mathrm{on})}{n_1(\mathrm{off})} = \frac{(1+n_{20}(\mathrm{on}))\sinh^2 gt}{(1+n_{20}(\mathrm{off}))\sinh^2 gt} = 1 + n_{20}(\mathrm{on}),$$
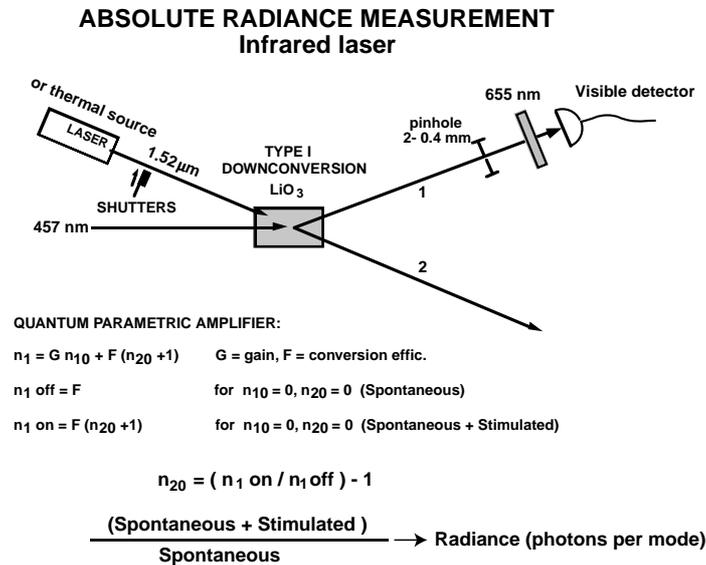
ABSOLUTE RADIANCE MEASUREMENT
Infrared laser

Fig. 9. – Measurement of the infrared laser spectral radiance (brightness) using vacuum fluctuations as a universal reference.

where $n_{20}(\text{off}) = 0$, and $n_{20}(\text{on}) \neq 0$. (Note: in our setup channel 1 is visible and channel 2 is IR.) This result allows an unknown radiance to be determined in the fundamental units of photons/mode.

6˙2. *Measuring the radiance of infrared light using correlated visible photons*. – To make practical use of these results to measure radiance it is necessary to be cognizant of several issues. First, the radiance (the ratio in eq. (24)) measured is that which is added to the crystal region being pumped by the laser, so any input losses must be accounted for. Second, the size of that pumped region is essentially the spatial resolution of the measurement, so it is useful to uniformly bathe that region with the field to be measured to avoid unwanted averaging. Similarly, it is necessary to angularly overfill the sensitive region. This angular extent is set by the phase-matching conditions of eq. (1) and the bandwidth of the measurement.

In our initial experiments to produce the correlated pairs of photons, a linearly polarized Ar+ laser, power-stabilized to 300 mW at 457.9 nm, was used to pump a LiIO$_3$ crystal (see fig. 9). The 15 mm × 15 mm × 10 mm long crystal was mounted in a housing purged with dry air to prevent moisture from fogging the surfaces. The crystal was cut with its optic axis inclined vertically at 33.6° to the input surface normal. The crystal itself was inclined to the pump direction so that the resulting angle between the optic axis and the pump beam within the crystal was 28°. This particular configuration produces correlated visible/infrared photon pairs with the visible photons emitted at $\sim 4°$ and the infrared photons emitted at $\sim 25°$ to $45°$ from the pump-beam direction. In

ABSOLUTE RADIANCE MEASUREMENT
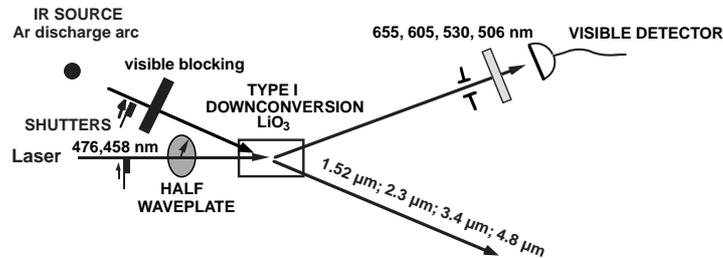**Broadband thermal radiation**

Fig. 10. – Calibration of spectral radiance of a broad band (high-temperature black-body model) infrared source.

addition to the energy and momentum requirements previously discussed, the polarization of the pump beam must be oriented parallel to the plane defined by the optic axis and the laser direction. This polarization orientation is required by the parametric down-conversion process defined as type I which, in our setup, uses pump radiation polarized as an extraordinary ray to produce down-converted photon pairs polarized as ordinary rays (perpendicular to the optic axis). A half-wave plate was used to orient the pump-beam polarization along the optic axis of the crystal, maximizing the down-conversion output. Similarly, by rotating the pump beam polarization 90°, the parametric down-conversion production can be turned off to allow for background subtraction. Shutters in both the pump beam and in the infrared source beam were also used to search for any non–down-converted light leakage into the detection system. All detection was carried out in the visible region. An EG&G SPCM-AQ-231 actively quenched thermoelectrically cooled Si avalanche photodiode (APD) was used to detect the presence of the visible down-converted light. A 25 mm focal-length lens was placed about 25 mm from the APD to concentrate the light.

We have carried out a detailed theoretical and experimental study of quantum parametric up-conversion for this purpose, both in the spontaneous and in the spontaneous-plus-stimulated (when radiation from the external infrared source is incident) regimes. We specifically studied the spatial geometry and statistical features of the process for the measurement of both thermal (fig. 10) and coherent (laser) (fig. 9) infrared radiation [22]. We expect to develop a technique for the evaluation of infrared-radiation color temperature, exploiting the fact that the radiance (brightness, or number of photons per mode) is directly related to Planck's thermal-radiation formula. Special efforts will be devoted in the near future to the design of a miniaturized version of our apparatus for the measurement of intensity of 1.5 mm wavelength radiation for telecommunications applications.

7. – **Quantum ellipsometry**

The recent research with type-II SPDC, where the signal and idler photons have mutually orthogonal polarizations, has shown that the double entanglement of such states both in space-time and in polarization [11, 12] can be used to develop even more sophisticated optical measurement techniques. This feature has already stimulated significant advances in quantum optics research. We are currently in the process of developing a new approach to the absolute measurement of optical delay between two orthogonally polarized waves in optical and photonic materials using quantum pairs of correlated polarized photons. Our enthusiasm is based on the previously demonstrated fact of superior performance and wider practical applicability of optical techniques based on the use of quantum principles.

This type of measurement is traditionally an area of optical ellipsometry. Conventional ellipsometry techniques were developed over the years to a very high degree of performance and are used every day in many research and industrial applications. Unfortunately, some limitations of principle exist in the nature of the classical optical states and in the way they are prepared and utilized.

Traditional (non-polarization) techniques for the measurement of optical delay usually make use of monochromatic light. The introduction of an optical sample in the one arm of the interferometer causes a sudden shift of interference pattern (sometimes over tens or hundreds of wavelengths) proportional to the absolute value of the optical delay. This approach requires one to keep track of the total number of shifted interference fringes to evaluate the absolute value of the optical delay. The accuracy of this approach is limited by the stability of the interferometer, the signal-to-noise level of the detector, and the wavelength of the monochromatic radiation used. Conventional polarization interferometers used in ellipsometry measurements provide very high resolution, but have a similar problem of tracking the absolute number of 2π shifts of optical phase during the polarization mode dispersion measurement. Optical engineers over the years have been able to come up with several ways to get around this problem using additional complex measurement procedures. The use of monochromatic classical polarized light does not allow one to measure the relative delay between two orthogonal waves in a single measurement. Several measurements at different frequencies are required to reconstruct the polarization dispersion properties of optical material. The use of highly monochromatic laser sources creates a problem of multiple reflections and strong irregular optical interference, especially in studying surface effects. Ellipsometry with low-coherence sources (white light) has received attention as a convenient method for the evaluation of dispersion parameters of optical materials in general, and of communication fibers in particular. While the technique provides the high timing resolution along with the absolute nature of the optical delay measurement, its suffers from the problem of low visibility and instability of the interference pattern. This usually limits the maximum possible resolution and accuracy.

We selected several problems known in applied ellipsometry of optical and photonics materials which can benefit the most from the use of new quantum principles.

7˙1. *Measurement of polarization mode dispersion with attosecond resolution.* – Down-conversion is called type I or type II depending on whether the photons in the pair have parallel or orthogonal polarization. The photon pair that emerges from the nonlinear crystal in down conversion may propagate in different directions or may propagate collinearly. The frequency and propagation directions are determined by the orientation of the nonlinear crystal and the phase-matching relations. Type-I SPDC has been used extensively as a convenient source of two-photon entangled states. The quantum correlations in type-I SPDC were used for practical radiometry applications even before they were recognized as a useful tool for the basic research in quantum mechanics. It was shown recently that type-II SPDC provides much richer physics due to the resulting two-photon entanglement both in space-time and in spin (polarization). Because of this double entanglement, it is possible to demonstrate Bell's inequality violations for both space-time and spin variables in a single experimental setup. The dispersion of the ordinary and extraordinary waves in a nonlinear crystal lead to a wave function space-time structure which is completely different from that generated in type-I SPDC. This unique double entanglement of the two-photon state in type-II SPDC provides us with ultimate control of the relative position of these two photons in space-time.

The study of polarization entanglement and of the natural rectangular shape of the two-photon wave function in space-time in type-II SPDC allows us to measure propagation time delay in optical materials with sub-femtosecond resolution. This technique provides much better time resolution, contrast, stability, and statistical accuracy than techniques based on the Type-I SPDC interferometers. By manipulating the optical delay between the orthogonally polarized photons a V-shaped correlation function is realized by a coincidence photon counting measurement [23]. The general principle and schematic experimental setup is illustrated in fig. 11.

The sharp V-shaped intensity correlation function can be made just 5-10 femtosecond wide. This notch shape is different from the classical Gaussian shape curve and allows us to evaluate the relative displacement on a time scale with higher resolution. The introduction of any additional sample of optical material or photonic device with different o-ray (u_o) and e-ray (u_e) group velocities in the optical path before the beamsplitter will shift the V-shape distribution on a sub-femtosecond time scale. This shift is proportional to the optical delay in the sample of the length L:

$$(25) \qquad \delta = (1/u_\mathrm{o} - 1/u_\mathrm{e})L \approx (n_\mathrm{o} - n_\mathrm{e})L/c.$$

This technique provides a direct measurement of the absolute value of total optical delay between two linear (circular, or any elliptical) orthogonally polarized waves inside a sample. This is rather different from conventional polarization measurements, where an optical delay can be evaluated only modulo to the one wavelength period. It has the advantage of practically 100% contrast as a result of noise suppression due to a quantum correlation measurement.

A 351 nm Ar$^+$ laser pumps the BBO crystal in a collinear and frequency-degenerate ($\omega_1 = \omega_2 = \frac{\omega_\mathrm{p}}{2}$) configuration. Pairs of orthogonally polarized photons generated in the

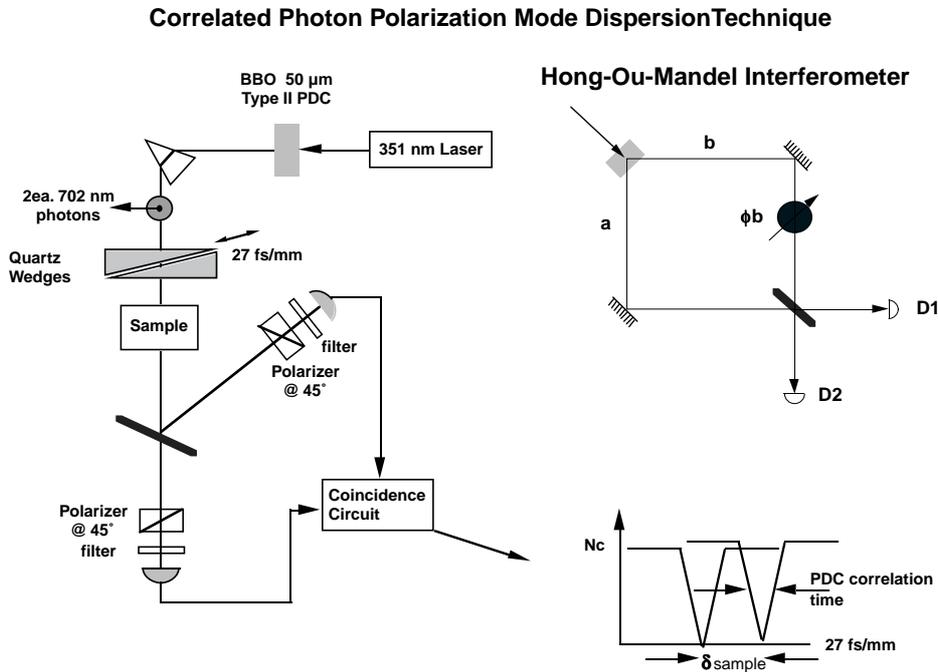**Correlated Photon Polarization Mode DispersionTechnique**

Fig. 11. – General schematic of a two-photon polarization interferometer.

BBO nonlinear crystal enter two spatially separated arms via a polarization-insensitive 50-50 beamsplitter (BS) so both ordinary and extraordinary polarized photons have equal probability to be reflected and transmitted. The two analyzers oriented at 45° A_1 (A_2) in front of each photon-counting detector D_1 (D_2) complete the creation of what are in essence two spatially separated polarization interferometers for the originally $X(Y)$-oriented signal and idler photons. Signal correlation is registered by detecting the coincidence counts between detectors D_1 and D_2 as a function of a variable polarization delay (PD) in the interferometer. Spontaneous parametric down-conversion in a BBO (β-BaB$_2$O$_4$) nonlinear crystal with $L = 0.05$ mm to 1 mm generates signal and idler photons with coherence lengths of tens to hundreds of femtoseconds. This idea is illustrated in fig. 12.

The new feature realized in our experiment is the non-symmetric manipulation of the relative optical delay τ between ordinary and extraordinary photons in only one of the two spatially separated interferometers. The observed coincidence probability shows a triangular envelope which is now filled with an almost 100% modulation associated with the period of pump radiation. The additional introduction of a sample of optical or photonic material with different o-ray (u_{o}) and e-ray (u_{e}) group velocities in the optical path before the beamsplitter shifts the interference pattern proportional to $\tau_{\mathrm{sample}} = d/c$ (see fig. 14), the difference in propagation times of the two polarizations. This allows us
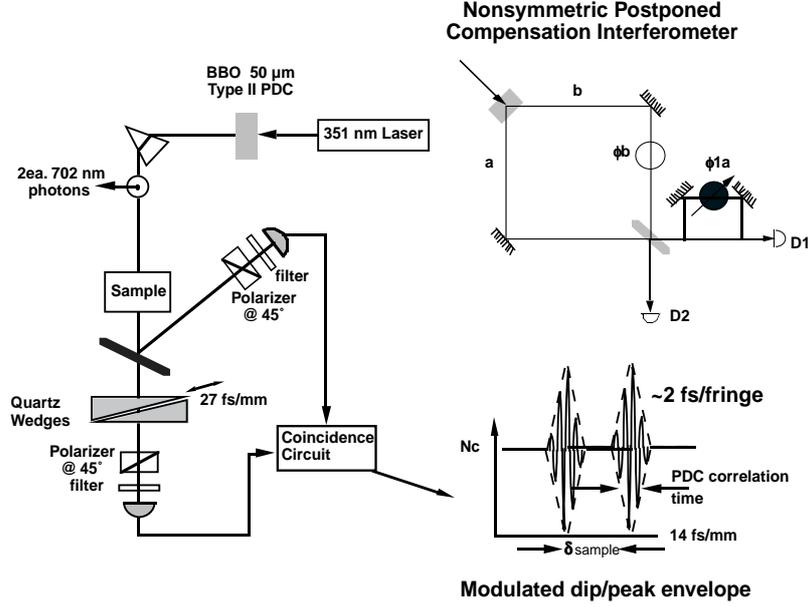
Fig. 12. – Schematic of a two-photon polarization interferometer with a postponed optical delay. This non-symmetric delay is introduced only in one arm after the beam splitter.

to measure directly the absolute value of total optical delay between two orthogonally polarized waves in the sample on a very fine sub-femtosecond time scale.

The experimental result of the measurement of intensity correlations (coincidence probability) as a function of relative polarization delay δ is illustrated in fig. 13. Unusual in classical optics is the triangular shape of the envelope that is a clear signature of a quantum character of this spontaneous parametric down-conversion. The SPDC signal is delivered to the detectors without the use of any limiting spectral filters. The full width at half-maximum (FWHM) of the correlation function envelope is defined by

$$(26) \qquad\qquad \delta = (1/u_{\mathrm{o}} - 1/u_{\mathrm{e}})L_{\mathrm{crystal}}.$$

The measured value of 66 fs corresponds to the spectral width of the phase matching in the 0.565 mm BBO crystal cut at 49.2° to its optical axis. The high visibility of the interference pattern and the extremely high stability of the polarization interferometer in such a collinear configuration allows us to identify the absolute shift of the wide envelope with an accuracy defined by the fringe size of an internal modulation. We would like to emphasize the very high contrast of observed quantum interference, $\sim 90\%$.

The resolution is further enhanced by reducing the total width of the envelope. This can be done by widening the phase matching spectrum by reducing the crystal length to $50\,\mu\mathrm{m}$. This arrangement was used to measure the optical delay of a crystal quartz sample introduced into the optical path before the beamsplitter BS. The result of this
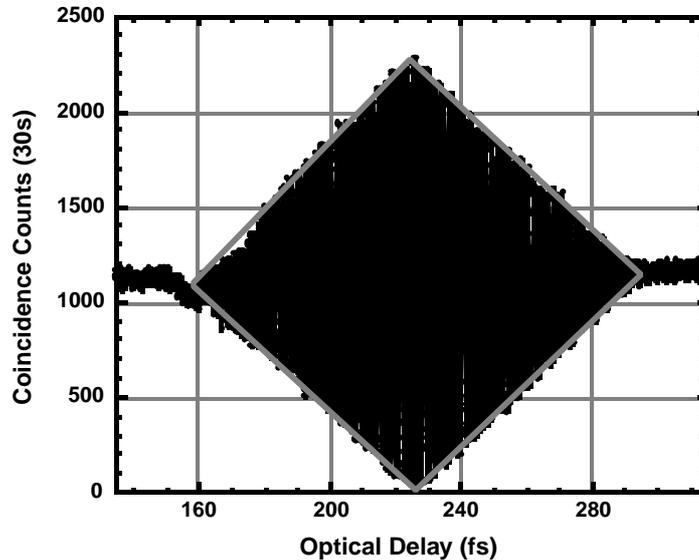
Fig. 13. – Observed quantum interference (intensity correlation) of entangled photons generated in a 0.565 mm long BBO crystal. All measurements are without any spectral alterations of original two-photon states.

measurement (performed with the $50\,\mu$m nonlinear crystal) is illustrated in fig. 14. The 25 fs width of the envelope enables us to clearly identify the central fringe position. Based on our signal-to-noise ratio we expect to resolve at least $1/100$ of a fringe $\sim (10^{-17}\,$s$)$.

We use results of our study and experimental setup to develop a practical technique for the characterization of properties of optical and photonic materials that are widely used in optical communication devices: optical fibers, switches, multiplexes, and fiber sensors.

The major advantage of this new technique over the traditional polarization ellipsometry is the direct measurement of the absolute value of group velocity dispersion between two basic polarization modes supported by the material. It provides sub-femtosecond time resolution for the measurement of polarization mode dispersion without using femtosecond laser sources. Quantum entanglement and correlation of two photons provide much higher contrast, stability, and accuracy than any conventional technique by eliminating the noise contribution. The low intensity and variable wavelength of the probe light makes it possible to have a continuous monitoring of major parameters of optical materials during their manufacture process or during their operation when any external forces or fields are applied. This approach has potential for the conversion of already installed fibers into the fiber sensors.

The following materials and devices could be characterized based on the use of this new technique:

a) Single-mode fibers are the main material in communication lines. Frequency dispersion in fibers has been greatly reduced by the industry over the last decade. Polarization
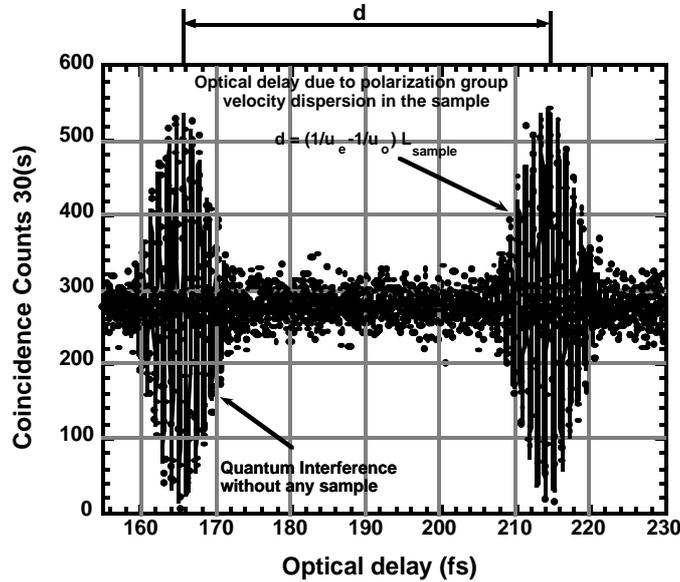
Fig. 14. – Measurement of the optical delay in the crystal quartz sample using a $50\,\mu$m nonlinear crystal. The horizontal scale is the time delay of the delay line located after the beamsplitter, BS. (The delay of the sample is one half that of the delay line.)

dispersion of fiber modes is now a major limiting factor in the increase of communication speed. This characteristic is extremely important for the manufacturers of communication fibers and especially for the soliton carrying fibers which are now being used for communication lines.

b) Polarization-preserving Hi-Birefringent fibers (Hi-Bi elliptical core fibers) which support only two polarization modes without mixing them. They are used intensively in modern laser gyroscopes for the navigation of aircrafts and missiles.

c) Nonlinear waveguides with different optical properties are major component of many optical devices used in communication such as switches and multiplexers.

d) Faraday rotators, optical isolators, organic optically active crystals such as sugar, glucose, and some more complex proteins and aminoacids. Our technique for the linear polarization dispersion measurement is easy convertible to the case of circular polarization. All advantages of using quantum correlation are valid.

This technique can be easily modified to study optical interactions at the surfaces of materials, as is illustrated in fig. 15. We will exploit a reflection configuration, rather than the transmission mode, and take advantage of the strong polarization dependence of evanescent waves. The polarization sensitivity and sub-femtosecond time resolution of the proposed technique, along with the smaller-than-wavelength scale of evanescent waves, promises that this method will provide new information about the electronic, optical, and structural properties of surfaces and thin films. Specifically, we believe that

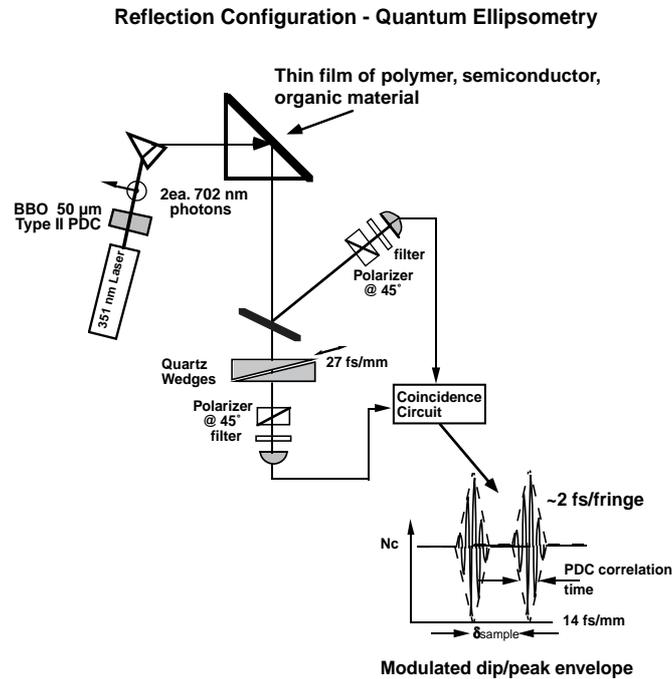**Reflection Configuration - Quantum Ellipsometry**

Fig. 15. – Schematic of the experimental setup for the polarization dispersion measurement between two orthogonally polarized waves reflected from a surface structure.

this approach is a uniquely sensitive tool for the analysis of the orientation, structure, morphology, and optical properties of single and multiple layers of atoms either grown or deposited on a substrate. Further, if the technique can be demonstrated to be sensitive to the chemical identity of adsorbed molecules and atoms, then we will explore the application of the method to the field of chemical sensors.

This technique also offers a novel approach to the study of the surface modification of photonic materials due to their structure, or physical conditions. This will be extremely important in characterizing major physical properties of modern structures for ultrafast photodetection such as quantum dots and clusters.

8. – Quantum metrology meets quantum information: quantum cryptography

Today's modern communication and information systems transmit a substantial amount of sensitive and financial information through both regular data networks and specialized channels. The level of communication security using traditional encryption tools depends on the computational intractability of mathematical procedures such as factoring large numbers. This approach is intrinsically vulnerable to advances in computer power. The explosion of new information services dictates a need for totally new and unconventional approaches to the problem of security and data authentication in

communication networks. The recent developments in experimental tests of fundamental problems of quantum mechanics such as Einstein-Podolsky-Rosen (EPR) paradox [24] and Bell's inequalities violation [25] have introduced a new paradigm for secure communications —quantum cryptography. The privacy of transmitted information can now be protected by the fundamental laws of nature.

Quantum cryptography is based on two major techniques that utilize the quantum nature of photon state. One approach makes use of single-photon states prepared from light in a coherent state [26]. It has a major drawback based on the statistical fluctuations of the number of photons in the original state. This adds the possibility of having two photons simultaneously in the communication channel. An eavesdropper can use one to extract partial information. The other approach is based on the non-local character of two-photon entangled (EPR) states generated in the nonlinear process of spontaneous parametric conversion (SPDC) [27]. The unique correlation of two photons in space, time, energy, and momentum resolves the previous problem. Unfortunately, the applicability of the latter technique has been severely limited because of the low visibility and poor system stability inherent in the use of type-I SPDC and the need for the synchronous manipulation of two Mach-Zehnder interferometers that are well separated in space.

Based on our previous experimental results and experience in quantum optics research, we have become aware that the use of doubly entangled EPR states generated by type-II SPDC provides a much more flexible, robust, and reliable quantum apparatus for cryptography. The high contrast and stability of the fourth-order quantum interference patterns demonstrated in our initial experiments promise to bring the performance of EPR-based quantum cryptography systems up to the level of the best single-photon systems.

The key feature of quantum cryptography, the impossibility of cloning the quantum state or extracting information without destroying it, carries with itself a major limitation on the distance of secure information transfer. This limit is the distance that a single-photon state can travel without absorption. It is as a matter of principle impossible to amplify the quantum state. The level of signal attenuation in modern fibers currently poses a limit of 15-20 km for a reliable quantum cryptography. The open-air communication may be more feasible especially when fibers are not available (ship-to-ship, or in-field communication). The problem of secure communication to a satellite is also one of the most vital issues in modern telecommunication. Ground-to-satellite, satellite-to-satellite, and satellite-to-ground communication becomes even more important when communication links must go over the horizon. Open-air quantum cryptography will become a crucial tool in these situations. The thickness of the atmospheric layer is just several kilometers and its density rapidly decreases with altitude. Satellite-to-satellite communications using our cryptographic method in space will have only one problem to solve: how to point and to collimate the beam. Finally, the synthesis of both approaches —local distribution over the fiber lines and transmission over the horizon using satellite-based links— can provide a global secure communication network.

Our experimental efforts include the laboratory modeling and outdoor testing of the open-air cryptographycally protected line. The emphasis is on the study of the influ-

ence of atmospheric effects and the possibility of day-time operation. The development of a fiber-based communication channel prototype includes detailed studies of polarization mode dispersion in communication fibers, including single-mode and polarization-preserving fibers. We also study the possibility of utilizing a rather remarkable effect of dispersion cancellation that was shown in earlier quantum optics experiments. This unusual effect occurs when a twin-beam quantum interferometer contains dispersive materials. Special efforts are directed towards designing and building a compact source of entangled photons suitable for practical use in communication lines.

We have shown recently that the use of high-repetition-rate femtosecond pulses significantly enhances the flux of entangled-photon pairs available for reliable and secure key distribution. The down-converted entangled pairs appear only at those well-defined times when pump pulses are present (repetition rate ~ 80 MHz). This provides narrow windows where coincidences can be obtained —separated by fixed time intervals during which the detectors can recover— thereby significantly enhancing the overall coincidence rate. We are currently exploring the possibility of miniaturizing the femtosecond laser source and incorporating it in the practical model of secure channel.

8˙1. *Practical concepts of quantum cryptography*. – There are two conceptual models that allow us to understand the underlying principle and the technical challenge of quantum key distribution (QKD). First there is the orthodox view of quantum measurement which states that any measurement of a quantum system collapses the quantum state of the system onto one of the specific states characteristic of the measuring device. Accordingly, if an eavesdropper attempts to extract information about the state of the photon as it passes from one party to the next, the resulting detectable disturbance of the state allows the parties to disregard the key compromised generated by that photon. In this sense, we may regard the quantum channel as a long thin wire between the parties which immediately breaks if it is disturbed by an eavesdropper. Already we see two potential technical difficulties. First, if the signal is composed of more than one photon, an eavesdropper (let us call her Eve) may tap the line and gather one or more of the "extra" photons for measurement while not revealing her presence. Second, the effect of an eavesdropper measurement is indistinguishable from noise and thus if the noise in the channel is high or time-varying, Eve may disguise her measurements in the baseline noise of the undisturbed signal. Both of these concerns must be addressed.

The second model that can give us insight into QKD is that of a particle with two or more pathways available to it. By putting detectors on two of the pathways in two distinct experimental setups, we can calculate the probabilities, p_1 and p_2, of the particle taking either of the two paths. The novelty of quantum mechanics is that if we then make a measurement which signals only that the particle chose one of the paths *and gives no information about which path it took*, the probability of a signal can deviate from $p_1 + p_2$. In fact, by adjusting experimental settings which have no effect on either p_1 or p_2 individually, it is possible to make the probability vary between 0 and 1. This variation around $p_1 + p_2$ is controlled by the actions of both parties and thus the parties can use the experimental outcome to infer the actions of the other party, enabling them to

share a secret key. The technical difficulty highlighted by this scheme is the requirement that the measurement reveal no information about which path the particle took. Of course, it is not sufficient to ensure that the experimenter not receive any information about which path was followed; the crucial point is that *no one* must be able to extract any information about which path the particle took, even in principle. This means that any impediments, impurities or time-dependent parameter fluctuations in one of the paths that may register the passage of the particle will destroy the coherence of the two paths, preventing the variation of the joint measurement probability.

8$\cdot$**2.** *One photon or two?* – Experimental realizations of current quantum cryptosystems can be divided into two groups: those which rely on weak coherent single-photon states and those which rely on multi-particle entanglement. The weak coherent schemes are based on the protocols developed by Bennett and Brassard [26].

In these schemes one party prepares a single-photon state by attenuating a pulsed laser to obtain a photon count of ≈ 0.1 photons per pulse. The entanglement scheme developed by Ekert [27] involves the creation of a maximally entangled two-photon state (EPR state) and the measurement of the two particles by spatially distant parties.

The entanglement scheme has several inherent advantages over the weak coherent based scheme; however, the first attempts at implementing EPR QKD led to low visibility of the specifically quantum effect and thus the method was discarded. Since then, weak-coherent-state QKD technology has progressed so that a thousand bits per second can be securely shared between sites 50 kilometers apart. Despite this success, a novel approach to EPR QKD described below promises to overtake weak-coherent-state–based technology.

8$\cdot$**3.** *Advantages of using EPR pairs.* – In the weak-coherent-state implementations, a laser pulse train with randomly distributed photon occupation is attenuated to achieve a high probability of 0 or 1 photons per transmitted pulse. In determining the degree of attenuation, there is a tradeoff between the bits of key per second shared and the probability that a transmitted laser pulse may contain 2 or more photons. Since a multiple-photon pulse is vulnerable to undetected monitoring (by the use of a beamsplitter), the attenuation is usually increased until the probability of two photons is on the order of 0.01. This normally means that only one in ten pulses transmitted by the attenuator has a photon, thus reducing the possible communication rate by an order of magnitude. In EPR QKD, each photon created and measured is accompanied by exactly one other perfectly synchronized photon, preventing any attempts at undetected beamsplitting. Furthermore, in EPR QKD the detector at the first party activates (via an authenticated message over a public line) the second party's detector for a short temporal window, enabling the rate of false detection to be brought down to an acceptable level, making EPR QKD ideally suited for free space transmission during daylight.

A second problem with coherent state QKD is that, since the arrival of photons at the second party's detector is governed by a random process, the active optical elements used

to create the shared key must be connected to the fiber throughout the transmission. This makes them vulnerable to probe beams injected by an eavesdropper in order to determine the classical state of lasers, polarizers and phase modulators. Since the second detector in the EPR QKD is triggered for only a short duration by the response of the first detector, the eavesdropper is unable to reliably determine the classical settings of the optical elements at the precise time of the coincident detections.

It should be noted that, while EPR QKD is distinguished from weak-coherent-state QKD by its inherent security advantages, both techniques can be seen as single photon state preparations and measurements. The reason is that although we regard them as different particles, the pair produced in EPR QKD is considered by quantum mechanics to be one object, and thus when the first measurement is made, the state of the other photon collapses immediately onto an eigenstate of the first measuring device. Thus, we may regard the two techniques as single quantum state generators, distinguished primarily by the superior timing control and eavesdropping-protection available in the EPR QKD scheme.

$8\dot{}4$. *Previous attempts to develop the quantum cryptography with EPR states*. – Experimental attempts to develop quantum cryptography with entangled-photon pairs (EPR states) had been initiated immediately after the main idea was introduced by Ekert [27]. This approach requires the use of a Franson-type interferometer [28]. This is a distributed system of two interferometers well separated in space with synchronously varied optical delay. Non-locality of the quantum features imbedded in the EPR pair should cause an almost 100% visibility of quantum interference observed in coincidence between detectors at the output of each interferometer. However, practical attempts to demonstrate the feasibility of quantum cryptography with EPR photons in fiber were not very successful. The applicability of this technique has been severely limited because of the low visibility inherent in the need of synchronous manipulation of the two spatially separated Mach-Zehnder interferometers.

$8\dot{}5$. *Demonstration of the new approach*. – The type-II SPDC provides a richer tool due to the two-photon entanglement both in space-time and in spin (polarization). The dispersion of the ordinary and extraordinary waves in a nonlinear crystal leads to a space-time structure of a wave function which is different from that generated in type-I SPDC. This unique double entanglement of the two-photon state in type-II SPDC provides us with control of the relative position of these two photons in space-time.

Polarization entangled photons are created by sending laser light through an appropriately oriented type-II second-order nonlinear crystal such as BBO (β-BaB$_2$O$_4$ or beta-barium borate). We used a collinear configuration of type-II SPDC and propagation of the down-converted light through a single-port beamsplitter.

To demonstrate that the EPR state is a reliable tool for quantum cryptography we employed a new approach using the non-local quantum interference of two-photon entangled states (EPR states) generated in type-II SPDC developed for the polarization mode dispersion measurement. It is based on the use of a *double, strongly unbalanced, and*
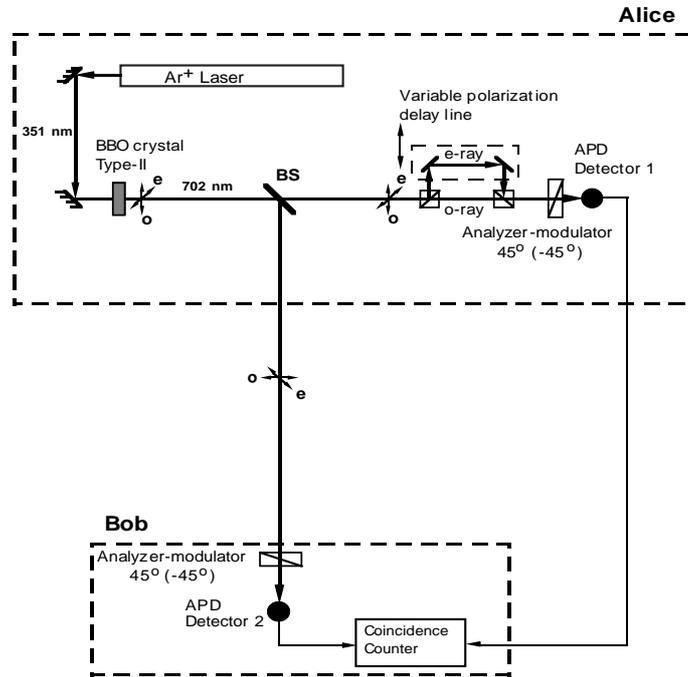
Fig. 16. – Schematic of the experimental setup for the generation of type-II entangled photons (with orthogonal polarization) and their registration using quantum interference with coincidence detection.

distributed polarization interferometer similar to the one we designed for the polarization mode dispersion measurement (see fig. 16).

The photons enter two spatially separated arms via a polarization-insensitive 50/50 beamsplitter (BS) allowing both ordinary and extraordinary polarized photons to be reflected and transmitted with equal probability. One arm contains a controllable polarization-dependent optical delay (the e-ray/o-ray loop). The introduction of polarization analyzers oriented at 45° in front of each photon-counting detector completes the creation of a polarization interferometer. Signal correlation is registered by detecting the coincidence counts between the two detectors as a function of the polarization delay.

This crucial features of this quantum interferometer are:

Double. One input beamsplitter (BS) and two output polarization beamsplitters (analyzers at 45 deg) well separated in space. A strongly unbalanced-polarization delay line is introduced only in one interferometer.

Distributed. First beamsplitter is with Alice, one of the output beamsplitters, is far away with Bob.

Non-local quantum interference. A phase shift imposed on one of the entangled photons does work for both of them even though they are well separated in space.

Polarization interferometer. We use a type-II SPDC and polarization analyzers at the output beamsplitter.
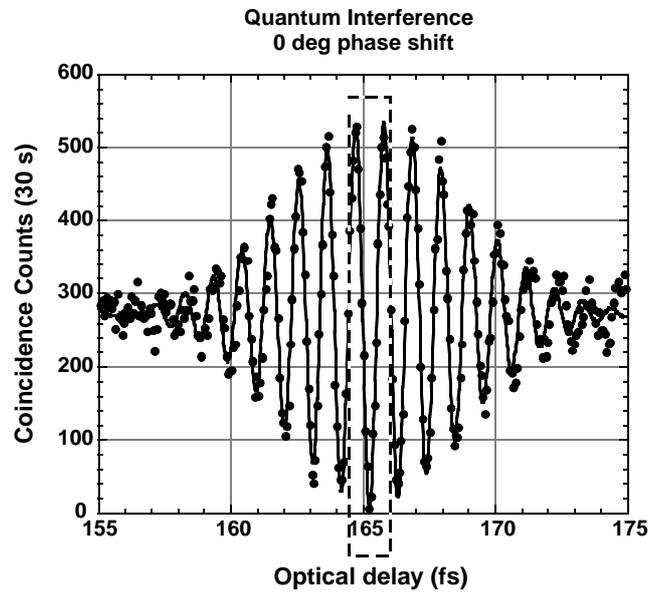
**Quantum Interference
0 deg phase shift**

Fig. 17. – Experimentally observed *destructive* interference at **0°** phase shift between polarization analysers.
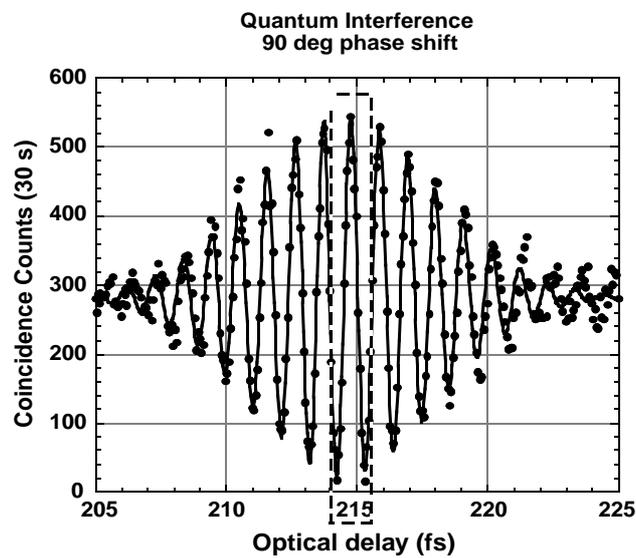
**Quantum Interference
90 deg phase shift**

Fig. 18. – Experimentally observed *constructive* interference at **90°** phase shift between polarization analysers.

Intensity correlations. Measure an intensity correlation function by detecting the variation in the coincidence counting rate.

The 90° shift of the phase in one of the analyzers will change the quantum interference immediately to be constructive in the central fringe (see fig. 18) with a very high ($\sim 99\%$) contrast.

Results shown in fig. 17 and fig. 18 demonstrate that the use of a polarization intensity interferometer in contrast to spatial interferometers in type-I SPDC provides much higher contrast (visibility of quantum interference dip) and stability with regard to mechanical and other external perturbations.

In order to complete the procedure of quantum key distribution using our new design, we have to randomly modulate the polarization parameters of the two-photon entangled state by switching each analyzer-modulator between two sets of polarization settings 0°/90° or 45°/135°. This can be accomplished using a fast Pockels cell polarization rotators in front of detectors. Using public communication line we then can proceed with one of the standard quantum cryptography protocols described in the literature [26, 27].

Our initial study has shown [29] that the phase-sensitive quantum interference of two entangled photons in strongly unbalanced polarization intensity interferometer delivers robust quantum hardware suitable for practical quantum cryptography applications. The high contrast and stability of quantum interference demonstrated in our experiments surpasses the performance of the best single-photon polarization techniques without their specific week points.

$$* * *$$

I would like to express my great thanks to long-term colleagues, collaborators, and friends: D. Klyshko, A. Penin, C. Alley, B. Phillips, A. Migdall, R. Datla, A. Parr, G. Jaeger, M. Teich and B. Saleh who have inspired, supported, and participated in the development of these exciting quantum metrology techniques over the last two decades.

REFERENCES

[1] Ou Z. Y. and Mandel L., *Phys. Rev. Lett.*, **61** (1988) 50.
[2] Shih Y. H. and Alley C. O., *Phys. Rev. Lett.*, **61** (1988) 2921.
[3] Hong C. K., Ou Z. Y. and Mandel L., *Phys. Rev. Lett.*, **59** (1987) 2044.
[4] Kwiat P. G., Steinberg A. M. and Chiao R. Y., *Phys. Rev. A*, **47** (1993) 2472.
[5] Brendel J., Mohler E. and Martienssen W., *Phys. Rev. Lett.*, **66** (1991) 1142.
[6] Larchuk T. S., Campos R. A., Rarity J. G., Tapster P. R., Jakeman E., Saleh B. E. A. and Teich M. C., *Phys. Rev. Lett.*, **70** (1993) 1603.
[7] Rarity J. G. and Tapster P. R., *J. Opt. Soc. Am. B*, **6** (1989) 1221.
[8] Kiess T. E., Shih Y. H., Sergienko A. V. and Alley C. O., *Phys. Rev. Lett.*, **71** (1993) 3893.
[9] Shih Y. H. and Sergienko A. V., *Phys. Lett. A*, **186** (1994) 29.
[10] Sergienko A. V., Shih Y. H. and Rubin M. H., *J. Opt. Soc. Am. B*, **12** (1995) 859.

[11] Atatüre M., Sergienko A. V., Jost B. M., Saleh B. E. A. and Teich M. C., *Phys. Rev. Lett.*, **83** (1999) 1323.

[12] Atatüre M., Sergienko A. V., Jost B. M., Saleh B. E. A. and Teich M. C., *Phys. Rev. Lett.*, **84** (2000) 618.

[13] Malygin A. A., Penin A. N. and Sergienko A. V., *JETP Lett.*, **33** (1981) 477.

[14] Sergienko A. V. and Penin A. N., *Appl. Opt.*, **30** (1991) 3582.

[15] Klyshko D. N., *Photons and Nonlinear Optics* (Gordon and Breach, New York) 1988 (in Russian (Nauka, Moscow) 1980.

[16] Yariv A., *Quantum Electronics* (Wiley, New York) 1967.

[17] Saleh B. E. A. and Teich M. C., *Fundamentals of Photonics* (Wiley, New York) 1991.

[18] Klyshko D. N., *Sov. J. Quantum Electron.*, **7** (1977) 591.

[19] Migdall A., Datla R., Sergienko A. V, Orszak J. S. and Shih Y. H., *Metrologia*, **32** (1996) 479.

[20] Czitrovsky A., Sergienko A. V, Nagy A. and Jani P., *Metrologia*, **37** (2000) 7.

[21] Louisell W. H., Yariv A. and Siegman A. E., *Phys. Rev.*, **124** (1961) 1646.

[22] Migdall A., Datla R., Sergienko A. V., Orszak J. S. and Shih Y. H., *Appl. Opt.*, **37** (1998) 3455.

[23] Dauler E., Jaeger G., Muller A., Migdall A. and Sergienko A. V., *J. Res. NIST*, **104** (1999) 1.

[24] Einstein A., Podolsky B. and Rosen N., *Phys. Rev.*, **47** (1935) 777.

[25] Bell J. S., *Physics*, **1** (1964) 195.

[26] Bennett C. H. and Brassard G., *Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalor, 1984*, p. 175.

[27] Ekert A. K., *Phys. Rev. Lett.*, **67** (1991) 661.

[28] Ekert A. K., Palma G. M., Rarity J. G. and Tapster P. R., *Phys. Rev. Lett.*, **69** (1992) 1293.

[29] Sergienko A. V., Atatüre M., Jaeger G., Walton Z., Saleh B. E. A. and Teich M. C., *Phys. Rev. A*, **60** (1999) R2622.