Hyper-entangled states and free-space quantum cryptography

Alexander V. Sergienko[a,b], Mete Atatüre[b], Giovanni Di Giuseppe[a,c],
Gregg Jaeger[a], Bahaa E. A. Saleh[a], and Malvin C. Teich[a,b]

[a]Quantum Imaging Laboratory, Department of Electrical and Computer Engineering,
Boston University, 8 Saint Mary's Street, Boston, MA 02215, USA
[b]Department of Physics, Boston University, 8 Saint Mary's Street,
Boston, MA 02215, USA
[c]Istituto Elettrotecnico Nazionale Galileo Ferraris,
Strade delle Cacce 91, I-10153 Torino, Italy

ABSTRACT

We describe the development of a quantum key distribution (QKD) scheme based on ultrafast laser pumped sources of entangled photon pairs and the engineering of their entanglement properties. Though quantum entanglement has been shown to be a useful resource for quantum key distribution, little work has been carried out in making use of the full range of joint entanglement behavior present in hyper-entangled photon pairs. We consider the principal advantages of our QKD scheme in connection with the way it makes use of ultrafast laser pumped spontaneous parametric down-conversion and hyper-entanglement. In particular, we consider how polarization quantum interference may be modified by manipulating the spatial features of the down-converted light.

Keywords: Quantum optics, quantum interference, entanglement, single-photon correlation

1. INTRODUCTION

Modern communication and information systems transmit a substantial amount of sensitive and financial information through both regular data networks and specialized channels. Communication security using traditional encryption tools most commonly depends on the assumed computational intractability of certain mathematical procedures, such as factoring large numbers. This renders traditional encryption methods intrinsically vulnerable to sudden advances in computing power. The explosion of new information services increases the need for totally new and unconventional approaches to the problem of security and data authentication in communication networks. At the same time, cutting edge experimental studies that have verified quantum mechanics arising from the Einstein-Podolsky-Rosen[1] paradox, such as measuring violations of Bell's inequalities,[2] have provided the tools for an emerging new method of provably secure communication: "quantum cryptography." Through it, the privacy of transmitted information can be protected by the fundamental laws of nature, allowing physics to play the role of the traditional human "trusted courier" of traditional top-level cryptographic security methods, with superior characteristics such as insusceptibility to human coercion and light-speed key transmission.

The essential element of quantum cryptography, quantum key distribution (QKD), is also the most advanced form of quantum communication currently carried out in practice. QKD is the distribution of a secret key (random bit sequence) between two parties, usually called Alice and Bob, to be used later for encrypting and decrypting messages. The highest guaranteed level of security is obtainable by combining the quantum key with the only known guaranteed-secure method of cryptography: Vernam's one-time pad.[3] Since it is generally impossible to measure an unknown quantum system without altering it, eavesdropping on quantum communications introduces physical errors in the transmitted data, so that any bits thereby rendered insecure may be removed from the cryptographic key-bit stream, by a process known as key-sifting.

Further author information: E-mail: AlexSerg@bu.edu, Telephone: 1 617 353 6564

QKD experiments have so far used one of two physical systems to transmit the QKD signal: weak coherent states of the electromagnetic field or entangled photon pairs produced by the spontaneous down-conversion (SPDC) of laser photons by non-linear crystals. The latter approach has the advantages offered by the nonlocal character of polarization Bell-states generated by SPDC.[4,5] The strong correlation of photon pairs entangled in both energy-time and momentum-space eliminates the problem of excess signal photons faced by the coherent-state approach, in which the exact number of photons actually present in the communication line in a given time interval is uncertain. In the entangled-photon technique, one of the two of entangled photons is measured by the sender, confirming for the sender that the state contains only the appropriate single photon. It has thus become the experimentally favored technique. Several innovative experiments using entangled photon pairs to implement quantum cryptography were made in the time frame 1999-2000.[6–9]

The basic QKD protocols are the BB84 scheme[10] and the Ekert scheme.[4] The former uses a stream of single photons transmitted from sender "Alice," to receiver, "Bob," randomly prepared in one of four polarization states: 0, 45, 90, and 135 degrees with respect to a laboratory coordinate system. The Ekert protocol uses a stream of entangled photon pairs, six polarization orientations for each photon, and a Bell-type inequality for the pair. Under BB84, when an eavesdropper, "Eve," tries to obtain information about the polarization; she will introduce observable bit errors, which Alice and Bob can detect by comparing a representative subset of the generated keys. In the Ekert scheme, both Alice and Bob receive one particle of the entangled pair and perform measurements along at least three different polarizer orientations on each side: measurements along parallel axes are used for key generation, while those along oblique angles are used for security verification.

All proposed schemes rely on the transmission of single-photon states. The initial schemes for using entangled states constituted significant progress towards practical quantum cryptographic technology. However, they still face the most serious limitation of all quantum cryptographic schemes, whether they use weak coherent states or entangled photon states: the distance photons must propagate to transmit information between parties. This makes the possible applications of QKD different from those of classical cryptographic schemes. Specifically, although QKD uses a classical open communication line that can be arbitrarily long and monitored by an adversary, it also requires a channel geometrically limited to direct line-of-sight or fiber-optic channel over which single photon states travel, the extent of which is limited by attenuation. Communication between buildings in a city, between ships at sea, between ground and satellite, or between satellites in space, are therefore the most practicable.

In Section 2, we discuss in more detail the benefits of using entangled photons for quantum cryptography, particularly vis-à-vis security against eavesdropping and combatting distance limitations arising in the case of fiber-optic transmission. We then go on in Section 3 to explore the benefits of using a femtosecond pulsed-laser pump to create entangled-photon streams for QKD. Finally, in Section 4 we consider a quantum-engineering approach that may provide some advantages for performing quantum key distribution; it involves careful manipulation of the hyper-entanglement inherent in multi-photon states generated by femtosecond pumped SPDC.

2. ADVANTAGES OF USING ENTANGLED PHOTONS

There are two substantial benefits to using entangled photons for realizing quantum key distribution: an increase in the effective distances of transmission and an increase in quantum channel security.

The basis of quantum cryptographic security – the impossibility of cloning any quantum bit or extracting information without influencing the system – also leads to its greatest practical limitations. The distance of secure information transfer is limited by the distance the photons needed to carry a delicate quantum state can travel without absorption, since a copy of the state simply cannot be made. The level of signal attenuation in modern optical fibers currently places a transmission distance limit of roughly 50–100 km for reliable quantum cryptography. Open-air communication may be more feasible and is also required by mobile receivers. Ground-to-satellite, satellite-to-satellite, and satellite-to-ground communication becomes even more important when communication links must go over a horizon. The atmospheric layer is several kilometers thick, with a rapidly decreasing density with altitude, making ground-to-satellite communication attractive. Satellite-to-satellite QKD in the vacuum of open space has only the problems of collimation and direction of the light beam. Ultimately, a synthesis of both methods – local distribution through optical fiber lines and transmission over the horizon using a satellite-based link – will be required by any secure communication network having global reach. Heterogeneous networking is inevitable.

Furthermore, the failure of the experimental community to determine the technological capacity of the best eavesdroppers has made comparing the performance of competing implementations difficult. For example, the mean number of photons per pulse has somewhat arbitrarily been set in the vicinity of 0.1 by the majority of researchers. Since this mean value is not determined by maximizing the number of secure bits per pulse, there is no guarantee that any of the implementations are not operating sub-optimally. More significantly, recent work has shown that the choice of 0.1 photons per pulse makes all existing weak coherent pulse implementations insecure to an eavesdropper armed with foreseeable, if not presently available, technology. Since QKD is to be rendered secure by physical rather than technological limitations, this is a highly significant fact.

Two potential technical difficulties arise thus far in analyzing QKD security performance. First, if the signal involves more than one photon, the eavesdropper Eve may tap the line and gather one or more of the "extra" photons for measurement without revealing her presence. Second, the effect of an eavesdropper measurement is indistinguishable from noise and losses in the channel; if the noise and loss in the communication line is high or time-varying, Eve may hide her measurements within noise of the undisturbed signal. Implementations of QKD, based on weak coherent pulses (WCP) and correlated photon sources (CPS), have been previously investigated.[11] A third implementation (CPS/PNR) is a new design that combines the perfect photon-number correlation in spontaneous parametric down conversion (SPDC)[6] with recently developed photon-number resolving (PNR) detectors[12–14] to reduce the deleterious effects of unwanted multiple photons. This novel design offers a substantial advantage over the competing implementations, principally because it more closely approximates single-photon transmissions.[15]

Let us now place no limitations on the technological capacity of the eavesdropper, except to insist that she attack each pulse individually. It is broadly accepted that restricting Eve to such individual attacks does not prevent her from carrying out the optimal attack, since her techniques for gaining information about any two pulses amounts to learning information from each separately, as any two bits of the transmitted random-bit string are uncorrelated. It is also not necessary to have complete security for each pulse, since one may also use classical privacy amplification algorithms for distilling arbitrarily secure keys from partially secure bits. As long as a bound on the information leaked to the adversary can be inferred from measurable quantities, such as the observed error rate, Alice and Bob can recover a perfectly secure, shared key by the following two-step procedure: i) they first use traditional error-correcting methods to ensure they have the same key, ii) they then use generalized privacy amplification[16] to extract a shorter secure key from a longer key. The crucial quantity for QKD is therefore the fraction G of the raw bits shared by Alice and Bob that may be retained, so that they are certain they share the same key while Eve has negligible information about that key. The quantity G is sometimes called the "gain."

The quantity G depends on four factors: the observed error rate, $\bar{\epsilon}$; the probability that Alice's detector-triggered source indicates that a valid signal was created, p_s; the probability that Alice sends a multi-photon pulse, S_m; and the probability that a pulse sent by Alice leads to a successful detection by Bob, $p_{\exp}$. The dependence of G on $\bar{\epsilon}$ for the BB84 protocol faced with such an adversary is known,[17] and the more crucial dependence of G on p_s, S_m, and $p_{\exp}$ has more recently been determined.[18] One may write

$$\begin{aligned} G(\bar{\epsilon}; p_s; S_m; p_{\exp}) = \frac{1}{2} p_s\, p_{\exp} \Big\{ & - R_1 \log_2 \left[\frac{1}{2} + 2\bar{\epsilon}\, R_1 - 2(\bar{\epsilon}\, R_1)^2 \right] + \\ & +1.35 \left[\bar{\epsilon}\, \log_2 \bar{\epsilon} + (1-\bar{\epsilon}) \log_2 (1-\bar{\epsilon}) \right] \Big\} \end{aligned} \qquad (1)$$

where $R_1 = (p_{\exp} - S_m)/p_{\exp}$. This expression has been derived using the most conservative approach to the imperfections in Bob's apparatus: Eve has complete control over all of the errors, photon losses, background, and dark counts that occur in the optical channel and in Bob's detection unit.

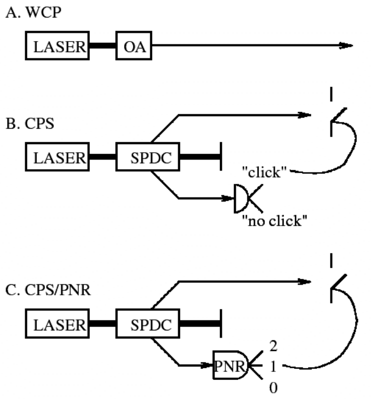

Figure 1. QKD source designs. A) A weak coherent pulse (WCP) from a laser source is optically attenuated (OA) to a mean photon number much less then one (the polarization rotator necessary for implementing the BB84 protocol is not shown). Panels B) and C) both show correlated photon source (CPS) implementations based on spontaneous parametric down-conversion (SPDC), in which Alice allows the pulse in the signal beam to propagate to Bob only if her detector indicates that one photon arrived in the idler beam. B) The idler beam is monitored with a standard 'click'/'no click' detector. C) The idler beam is monitored with a photon-number resolving detector (PNR), which can discriminate between single- and double-photon arrivals. (After.[15])

A complete QKD implementation requires not only a physical apparatus, but also an operational protocol. Since BB84 is the only protocol for which there exists an agreed-upon method for calculating $G(\bar{\epsilon}; p_s; S_m; p_{\text{exp}})$, it has been used in our work[15] comparing of the performance of the three implementations: WCP, CPS, and CPS/PNR. The physical apparatus required for the BB84 protocol can be viewed as composed of three parts: the single-photon source, the optical channel, and the detection unit. We now consider each of these three implementations, in turn.

Weak Coherent Pulse (WCP). The simplest and most common technique for reducing the likelihood of a multi-photon pulse is to attenuate the weak coherent pulse from a laser(see Fig. 1A). Alice must adjust the mean photon number per pulse to balance two undesirable effects: useless zero-photon pulses and insecure multi-photon pulses. Once the pulse is created, Alice and Bob make use of standard optical components to modify, launch, transmit, collect, and measure the polarization of the optical pulse.[19–21]

Correlated Photon Source (CPS). Brassard *et al.*[22] have investigated the ability of an SPDC-based detector-triggered source to mitigate the security ramifications of multi-photon signals (see Fig. 1B). The perfect correlation in photon number in the signal and idler beams allows Alice to run the protocol only when her detectors on the idler beam indicate that one photon was sent to Bob along the signal beam. While the correlated photon source extends the range of permissible channel losses far beyond that allowed in the WCP case,[11, 22] the Poisson statistics for the number of pairs per pulse,[23] combined with the inability of standard detectors to distinguish single-photon from multi-photon events, lead to the persistence of the compromising multi-photon pulses.

Correlated Photon Source/Photon-Number Resolving Detector (CPS/PNR). It is assumed in this case that Alice possesses a photon-number resolving detector, such as the state-of-the-art detector reported by Kim *et al.*[13] or by Cabrera *et al.*.[14] While this detector has a finite quantum efficiency (perhaps 70%), the gain mechanism ensures that the device can distinguish the number of incident photons with low error ($\approx 0.63\%$ for the device reported in Ref.[13]). The relatively high dark count rate (104 counts/sec for the device reported in Ref.[13]) can be countered by limiting the detector's exposure time by nanosecond gating. By initiating a pulse transmission only when the detector reports one photon arriving, Alice significantly reduces the fraction of pulses sent to Bob that contain more than one photon. However, extreme conditions are necessary for the PNR to provide such high efficiency and low multiplication noise.[13] Nonetheless, it provides a sign-post for future possibilities of this approach.

We have recently carried out a comparison of the performance of these three implementations over both free space and fiber-optic channels,[15] using values for optical coupling efficiency, error probabilities, and detector performance reported in the literature.[19–21] In each case, the performance was determined by maximizing the quantity G over the power of the original laser pulses that are either attenuated (for WCP) or down-converted (for the CPS and CPS/PNR implementations) to create the pulse. This step is important: lack of attention to it in prior considerations has led to unrealistic claims concerning secure bit rates. For a distance $d = 1$ km using a base repetition rate of 100 MHz, the CPS/PNR implementation offers a perfectly secure channel supplying 400 kbits/sec. This estimated transmission rate is approximately one order of magnitude greater than that offered by the WCP and CPS implementations. Using the rough estimates provided in Ref.,[21] we also simultated the gain achievable with each implementation for a range of low-Earth-orbit altitudes. While the WCP and CPS implementations do not offer secure communications at standard orbital altitudes, the CPS/PNR implementation could yield on the order of 1000 secure bits for each several minute night-time line-of-sight exchange using a 10-MHz repetition rate and a 300-km orbit.

Thus, there are two substantial benefits to using entangled photons for realizing quantum key distribution: an increase in the effective distances of transmission and increased quantum channel security. Our scheme supplements these advantages with others that arise from the use of an ultrafast laser pump for our system, as we discuss next.

3. ADVANTANGES OF USING ENTANGLED PHOTONS GENERATED BY FEMTOSECOND PUMPED SPDC

Our initial scheme[6] was the first of several experiments investigating the use of SPDC for QKD.[6–9] It demonstrated a flexible and robust QKD method using photon pairs generated via type-II phase-matched spontaneous parametric down-conversion (SPDC), through the use of a highly stable interferometric arrangement and a femtosecond pulsed laser pump. The approach benefits from the high visibility and stability of the resulting fourth-order quantum interference patterns. Since the intervention of any classical measurement apparatus (for eavesdropping) into the two-photon interferometer causes an immediate reduction of an initial 100% visibility (no eavesdropping) to 70.7% ($= 1/\sqrt{2}$ with eavesdropping), high visibility is required to ensure key security. Earlier work with entangled-photon QKD used type-I phase-matched pairs and, as a result, suffered from low visibility (only up to 85% without eavesdropping) and poor stability of the intensity interferometer, primarily due to the need for the synchronous manipulation of interferometers at substantial distances from each other in space. As a result, the ability to detect an eavesdropper, on which the security of quantum cryptography is based, was in danger of compromise.

Entangled states are those quantum states of multiple particles that cannot be written as a product of states for each of the particles individually.[24] Investigations of fundamental issues of quantum mechanics[1,2] have centered on the correlations of particle properties inherent in these states. Photon pairs (two-photons) created in the nonlinear process of SPDC[25,26] have been of sufficient quality to allow such investigations to reach their goals.[27] In SPDC, a pump laser beam is directed into a birefringent crystal, the nonlinear optical properties of which lead to the spontaneous emission of pairs of correlated photons. Entanglement in wavevector-frequency space (or, equivalently, space-time) can thereby arise from the phase-matching (*i.e.*, energy and momentum conservation) conditions:

$$\mathbf{k}_1 + \mathbf{k}_2 = \mathbf{k}_p \qquad\qquad \omega_1 + \omega_2 = \omega_p \ , \tag{2}$$

where the $\mathbf{k}_j$ are wave-vectors and the ω_j are frequencies, linking the input pump (p), and output photons (1 and 2). Phase matching in down-conversion is called type-I or type-II depending on whether the generated have parallel polarizations or orthogonal polarizations, respectively. The photon pairs emerging from the nonlinear

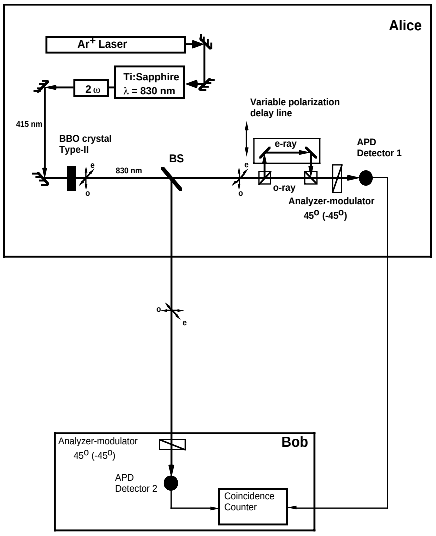

Figure 2. Schematic of the femtosecond two-photon entangled state QKD scheme. (After.[6])

crystal in general propagate either in different directions, but they may propagate collinearly as well. The frequency and propagation directions of the down-converted photons are determined by the orientation of the nonlinear crystal and the phase matching conditions. The state of the photon pair produced by SPDC is denoted $|\Psi^{(2)}\rangle$.[28]

The use of high-repetition-rate femtosecond pump pulses for down-conversion significantly enhances the production rate of entangled photon pairs,[28] and hence increases the rate of key distribution beyond the alternative entangled-photon approaches. Furthermore, down-conversion entangled pairs appear only at those well-defined times when femtosecond laser pump pulses are present (with a repetition rate of $\sim$ 80 MHz). This provides narrow time windows where coincidences can be obtained, separated by fixed intervals during which the detectors can recover, thereby significantly enhancing the overall coincidence rate and the flux of entangled-photon pairs available for reliable and secure key distribution.

In our proof-of-principle demonstration,[6] a frequency-doubled femtosecond Ti:sapphire laser was used to generate 80-fsec duration pulses at a wavelength of 415 nm that were sent through a 0.1-mm-thick BBO crystal oriented so as to yield collinearly propagating, type-II phase-matched EPR pairs (see Fig. 2). The dispersion of the ordinary (o) and extraordinary (e) waves in nonlinear crystals lead to a state space-time structure that provides control of the relative positions of the two orthogonally polarized photons. As mentioned above, interference visibility is the most crucial element of our QKD scheme. We thus used two polarization interferometers well-separated in space and synchronously varying the optical delays within and, hence, between them. The down-conversion photons entered the two spatially separated interferometer arms via a polarization insensitive 50/50 beam-splitter (BS), allowing both ordinary and extraordinary polarized photons to be reflected and transmitted with equal probability. One arm contained a controllable polarization-dependent optical delay (the e-ray/o-ray loop) and polarization analyzers in front of each photon counting detector were oriented at 45 degrees relative to the lab frame of reference.

The nonlocal quantum correlations of the two-photons we produced allowed a nearly 100% fourth-order quantum interference visibility to be obtained in coincidence between detectors at the outputs of these interferometers. Correlations were registered by detecting the coincidence counts between the two detectors as a function of the optical delay between orthogonally polarized photons. The first beam-splitter was located with the quantum key sender, Alice, and one of the output beam-splitters was far away with the receiver, Bob (see Fig. 2). Destructive quantum interference was observed at a 0 degree phase shift between the two polarization analyzers (see Fig. 3). The resulting interferogram that arises is characterized by two factors.[6] First, the

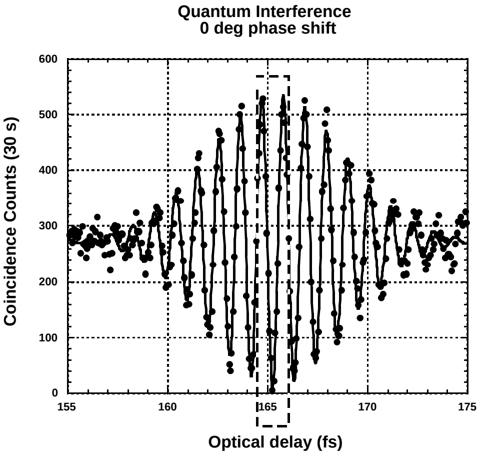

Figure 3. Coincidence interferogram obtained using the BBO nonlinear crystal and 80-fs pulsed laser pump. Destructive interference, corresponding to a binary "0," is observed when the relative polarization phase shift is 0 degrees. (After.[6])

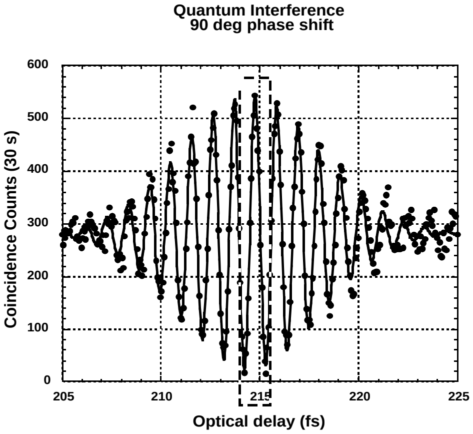

Figure 4. Constructive interference, corresponding to a binary "1" at 90 degrees relative polarization phase shift. (After.[6])

full-width at half-maximum of the envelope defines the coherence time,

$$T_{\text{coh}} \propto \left(\frac{1}{u_o} - \frac{1}{u_e} \right) L_c \ , \tag{3}$$

where u_o and u_e are the group velocities of the ordinary and extraordinary waves, respectively, and L_c is the length of the crystal.

In this scheme, the polarizations of the photons are then randomly modulated by switching each analyzer-modulator between two sets of polarization settings 0°/90° or 45°/135°. This is accomplished using fast

Pockels-cell polarization rotators in front of the detectors. The mutual measurement by Alice and Bob are thus destructive (a binary "0" as shown in Fig. 3) or constructive (a binary "1" as shown in Fig. 4) with 50%-50% probability, depending on relative orientation of modulators on the two sides. Communication between Alice and Bob over a public communication channel disclosing the set of polarizer orientations selected during measurement, but not the measurement outcome, is then sent, completing the standard quantum key distribution described in a literature.[17,19,20] The high-frequency carrier residing under the resulting HOM-type interference feature (Figs. 3 and 4) arises from the nonlocal entanglement of the twin beams. A 90 degree phase shift of one of the analyzers modifies the quantum interference pattern so that the central fringe is constructive rather than destructive (Fig 4). This demonstrates that a QKD signal – one value corresponding to each of the two sorts of interference – can be reliably encoded using this apparatus.

Implementations using entangled photons produced by femtosecond-pumped SPDC are therefore good candidates for practical implementation of the basic elements of quantum information networking, such as entanglement swapping, privacy amplification, quantum teleportation, and entanglement purification. With this basic ultrafast QKD scheme in place, we are now in a position to advance it further via the engineering of hyperentangled states,[29] as described in the next section.

4. HYPER-ENTANGLED STATE ENGINEERING FOR FREE-SPACE QUANTUM CRYPTOGRAPHY

The femtosecond pulsed pump entangled-photon QKD scheme at Boston University is now being improved by engineering various features of the hyperentangled photons produced by our entangled-state source. Recall that, in the nonlinear-optical process of SPDC in which a laser beam illuminates a nonlinear-optical crystal, pairs of photons are generated in a state that is jointly entangled in frequency, momentum, and polarization. A significant number of experimental efforts designed to verify the entangled nature of such states have been carried out using *single-variable* entanglement, such as entanglement in energy,[30] momentum,[31] or polarization.[32] Any attempt to access the features of one of the functions is affected by the presence of the others. As a result, the mainstream approach to investigating quantum interference to date has been to eliminate the dependence of the quantum state on entanglement involving parameters other than the one under consideration. For example, when investigating polarization-based entanglement, strong spectral and spatial filtering are typically imposed in an attempt to restrict attention to polarization alone. However, filtering leads to undesirable substantial losses of states available for quantum communication.

A different approach to this problem, which we expouse here, is to make practical use of the multi-parameter entangled (hyper-entangled) quantum state present at the outset. Our entanglement-control method uses the prescribed redistribution of quantum probability amplitudes, providing entangled-state engineering without filtering. We have shown both experimentally and theoretically[29] that the modulation of polarization entanglement resources (for example, polarization Bell-states) can be carried out by an appropriate manipulation of wave-vector and frequency components of two-photon states generated via the SPDC process. In this way, we garner the possibility of sending quantum key bits using several source parameters. Our initial proof-of-principle experiments along these lines were first performed using a cw laser pump; however this technique is applicable for femtosecond QKD, as well.

In particular, we have been investigating how an interferogram that exhibits interference in one variable such as polarization (one of the main parameters in existing quantum cryptographic techniques) can be modified at will by controlling the state via the other variables, such as transverse wave-vector or frequency.[29] The polarization used in our QKD scheme, for example, which is described as a function of relative temporal delay between the photons of an entangled pair, was observed to undergo substantial changes as the optical system was modified using different kinds of spatial apertures. Such interference maxima and minima can therefore be reached by this alternative path. This is an important observation in the context of quantum key distribution.

To understand how this effect can be precisely controlled, we must look in detail at the full two-photon state and its evolution within the optical system. It is helpful to view the experiment as proceeding through three distinct stages: the generation, propagation, and detection of the quantum state.[33,34] The quantum state at the output of the nonlinear crystal can be written as[29]:

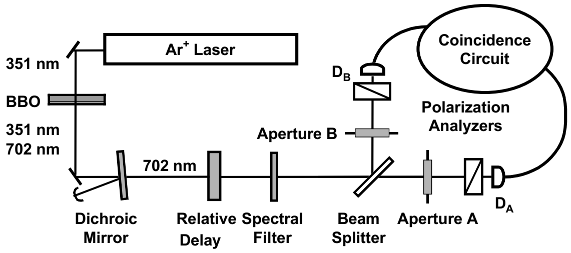

Figure 5. Schematic of experimental setup for observation of quantum interference using cw-pumped type-II collinear SPDC and shifted apertures. The configuration illustrated here makes use of a dichroic mirror to remove the residual pump radiation thereby admitting a large acceptance of the transverse-wave components. The dichroic mirror reflects the pump wavelength while transmitting a broad wavelength range that includes the bandwidth of the SPDC. The usual single aperture is replaced by two movable seperate apertures placed equal distances from the beamsplitter in each arm of the interferometer. (After.[29])

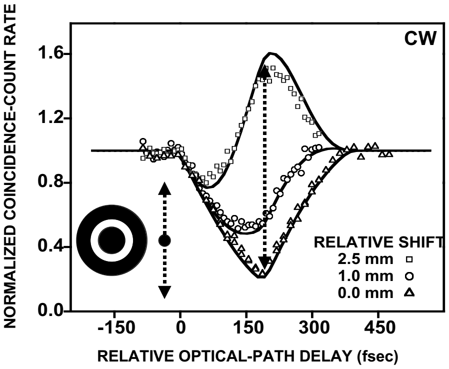

Figure 6. Normalized coincidence-count rate as a function of the relative optical-path delay, for an annular aperture (internal and external diameters of 2 and 4 mm, respectively) in one of the arms of the interferometer in the configuration of Fig. 5. A 7-mm circular aperture is placed in the other arm. The data were obtained using a 351-nm cw pump and no spectral filters. The symbols are experimental results for different relative shifts of the annulus along the direction of the optical axis of the crystal (vertical). The solid curves are the theoretical plots without any fitting parameters. (After.[29])

$$|\Psi^{(2)}\rangle \sim \int d\mathbf{q}_o d\mathbf{q}_e \, d\omega_o d\omega_e \; \Phi(\mathbf{q}_o, \mathbf{q}_e; \omega_o, \omega_e) \hat{a}_o^\dagger(\mathbf{q}_o, \omega_o) \hat{a}_e^\dagger(\mathbf{q}_e, \omega_e) |0\rangle \,, \tag{4}$$

with the state function

$$\Phi(\mathbf{q}_o, \mathbf{q}_e; \omega_o, \omega_e) \;=\; \tilde{E}_p(\mathbf{q}_o + \mathbf{q}_e; \omega_o + \omega_e) \, L \, \mathrm{sinc} \left(\frac{L\Delta}{2} \right) e^{-\mathrm{i}\frac{L\Delta}{2}} \,. \tag{5}$$

The operators $\hat{a}_j^\dagger(\mathbf{q}_j, \omega_j)$ serve as raising operators for the $(\mathbf{q}_j, \omega_j)$ modes, operating on the initial vacuum state $|0\rangle$. The quantity $\tilde{E}_p$ is the complex amplitude profile of the field, the $\mathbf{q}_j$ are the transverse momenta, L is the thickness of the crystal, and $\Delta = \kappa_p - \kappa_o - \kappa_e$, where the wavenumbers κ_j $(j = p, o, e)$ are related to the refractive indices.[29]

The nonseparability of the function $\Phi(\mathbf{q}_o, \mathbf{q}_e; \omega_o, \omega_e)$ in Eqs. (4) and (5) is the hallmark of *joint* multiparameter entanglement.[29]

Propagation between the planes of generation and detection is characterized by the transfer function of the optical systems (described by several quantities $\mathcal{H}_i$), which contain the impulse response function of the diffraction-dependent elements from the crystal output plane to the $i-$detector input plane. This approach has been developed in great details in our quantum-imaging studies.[29, 33, 34]

The formulation of the *detection* process requires some knowledge of the detection apparatus. Slow detectors, for example, perform temporal integration while detectors of finite area perform spatial integration. One extreme case is realized when the temporal response of a *point* detector is spread negligibly with respect to the characteristic time scale of SPDC, namely the inverse of down-conversion bandwidth. In reality all quantum-interference experiments typically make use of slow *bucket* detectors.[29]

The apparatus used in a series of recent experiments[29] is shown in Fig. 5. These experiments made use of a single-mode cw argon-ion pump laser with a wavelength of 351.1 nm and a power of 200 mW. The pump light was delivered to a β-BaB$_2$O$_4$ (BBO) nonlinear crystal with a thickness of 1.5 mm. The crystal was aligned to produce collinear and frequency-degenerate photon pairs by type-II SPDC. The collinear beams were then sent through a delay line comprised of a crystalline quartz element (with its fast axis orthogonal to the fast axis of the BBO crystal), the thickness of which could be varied to alter the delay between the photons of a down-converted pair. The photon pairs were then sent to a non-polarizing beam splitter. Each arm of the polarization intensity interferometer following this beam splitter contained an aperture described by $p_i(\mathbf{x})$ (with $i = A, B$), a Glan-Thompson polarization analyzer at 45°, a convex lens to focus the incoming beam, and an actively quenched Peltier-cooled single-photon-counting avalanche photodiode detector (denoted D$_i$ with $i = A, B$ in Fig. 5). No spectral filtering was used in the selection of the photons for detection. The counts from the detectors were conveyed to a coincidence counting circuit with a 3ns coincidence-time window – correction for accidental coincidences was not necessary.

Our studies of polarization quantum interference, often used in quantum information processing, has revealed a strong dependence of the so-called Hong–Ou–Mandel dip on the character of the quantum state. This state, as indicated above, is governed in part by the nature of apertures that may be deliberately placed in the experimental apparatus, which serve to modulate the presence of transverse-momentum components. A simple increase in the size of a pair of symmetric irises, for example, provides greater wave-number accessibility and thereby modifies the shape of the interference dip.[29] Moreover, for asymmetric apertures, the observed quantum-interference pattern can exhibit oscillations.

The most dramatic modulation in the profile of the two-photon quantum interference pattern, perhaps, occurs for apertures that are symmetric but *shifted* (in the transverse plane). We have demonstrated, that with a shifted annular aperture, one can even reverse the sign of the coincidence rate. In Fig. 6, we show results of polarization coincidence measurement with polarization analyzers parallel to each other for a 7-mm circular aperture in one arm and an annular aperture having an outer diameter of 4 mm and an inner diameter of 2 mm in the other. For certain values of the birefringent optical-path delay (τ), the interference pattern inverts, exhibiting a peak rather than the familiar dip ordinarily expected in this type of experiment. Conventionally, a change of this kind is attained only by using polarization modulation either at the source (Alice) or at the detector (Bob). In short, by simply changing the relative shift of the apertures, we are able to change the resulting interference between two qualitatively opposite high-visibility polarization Bell-states behaviors, thereby allowing the transmission of quantum information via coincidence events jointly measured by Alice and Bob.

In conclusion we demonstrated that hyper-entanglement can be a highly flexible and useful tool for implementing quantum key distribution in free-space. It offers the possibility of altering entanglement in a particular dimension (such as polarization) by effecting modifications in another dimension (such as transverse wavevector).

REFERENCES

1. Einstein, A., Podolsky, B., and Rosen, N., *Phys. Rev.* 47, 777 (1935).
2. Bell, J. S., *Physics* (Long Island City, NY) 1, 1195 (1964).
3. Vernam, G., *J. Am. Institute of Electrical Engineers* XLV, 109 (1926).
4. Ekert, A. K., *Phys. Rev. Lett.* 67, 661 (1991).
5. Ekert, A. K., Palma, G. M., Rarity, J. G., and Tapster, P. R., *Phys. Rev. Lett.* 69, 1293 (1992).
6. Sergienko, A. V., Atatüre, M., Walton, Z., Jaeger, G., Saleh, B. E. A., and Teich, M. C., *Phys. Rev. A* 60, R2622 (1999).
7. Tittel, W., Brendel, J., Zbinden, H., and Gisin, N., *Phys. Rev. Lett.* 84, 4737 (2000).
8. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., and Zeilinger, A, *Phys. Rev. Lett.*, 84, 4729 (2000).
9. Naik, D. S., Peterson, C. G., White, A. G., Berglund, A. J., and Kwiat P. G., *Phys. Rev. Lett.* 84, 4733 (2000).
10. Bennett, C. H and Brassard, G., in Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.
11. Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C., eprint: http://xxx.lanl.gov/abs/quant-ph/9911054.
12. Teich, M. C., Matsuo, K., and Saleh, B. E. A., *IEEE Trans. Electron Dev.* ED-33, 1475 (1986).
13. Kim, J., Takeuchi, S., and Yamamoto, Y., *Appl. Phys. Lett.* 74, 902 (1999).
14. Cabrera, B., Clarke, R. M., Colling, P., Miller, A. J., Nam, S., and Romani, R. W., *Appl. Phys. Lett.* 73, 735 (1998).
15. Walton, Z., Sergienko, A. V., Atatüre, M., Saleh, B. E. A., and Teich, M. C., *J. Mod. Opt.* 48, 2055 (2001).
16. Bennett, C. H., Brassard, G., Crépeau, C., and Maurer, U. M., *IEEE Trans. Inform. Theory* 41, 1915 (1995).
17. Fuchs, C. A., Gisin, N., Griffths, R. B., Niu, C.-S., and Peres, A., *Phys. Rev.* A 56, 1163 (1997).
18. Lütkenhaus, N., *Acta Phys. Slovaca* 49, 549 (1999) [eprint: http://xxx.lanl.gov/abs/quant-ph/9910093].
19. Marand, C. and Townsend, P. T., *Opt. Lett.* 20, 1695 (1995).
20. Townsend, P. T., *IEEE Phot. Technol. Lett.* 10, 1048 (1998).
21. Buttler, W. T., Hughes, R. J., Kwiat, P. G., Lamoreaux, S. K., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M., *Phys. Rev. Lett.* 81, 3283 (1998).
22. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., *J. Cryptol.* 5, 1 (1992).
23. Larchuk, T. S., Teich, M. C., and Saleh, B. E. A., *Ann. N. Y. Acad. Sci.* 755, 680 (1995).
24. Schrödinger, E. , Naturwissenschaften 23, 807 (1935); 23, 823 (1935); 23, 844 (1935) [Translation: Trimmer, J. D., *Proc. Am. Phil. Soc.* 124, 323 (1980); reprinted in *Quantum Theory and Measurement*, edited by Wheeler, J. A. and Zurek, W. H. (Princeton University Press, Princeton, 1983)].
25. Harris, S. E. , Oshman, M. K., and Byer, R. L., *Phys. Rev. Lett.* **18,** 732 (1967); Magde, D. and Mahr, H., *Phys. Rev. Lett.* 18, 905 (1967).
26. Klyshko, D. N., *Photons and Nonlinear Optics* (Gordon and Breach, New York, 1988).

27. Ou, Z. Y. and Mandel, L., *Phys. Rev. Lett.* 61, 50 (1988); Shih, Y. H. and Alley, C. O., *Phys. Rev. Lett.* 61, 2921 (1988); Hong, C. K., Ou, Z. Y., and Mandel, L., *Phys. Rev. Lett.* 59, 2044 (1987); Ou, Z. Y. and Mandel, L., *Phys. Rev. Lett.* 61, 54 (1988); Kwiat, P. G., Steinberg, A. M., and Chiao, R. Y., *Phys. Rev. A.* 47, 2472 (1993); Brendel, J., Mohler, E., and Martienssen, W., *Phys. Rev. Lett.* 66, 1142 (1991); 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, 1603 (1993); Steinberg, A. M., Kwiat, P. G., and Chiao, R. Y., *Phys. Rev. Lett.* 71, 708 (1993); Hong, C. K., Ou, Z. Y., and Mandel, L., *Phys. Rev. Lett.* 59, 1903 (1987); Rarity, J. G. and Tapster, P. R., *J. Opt. Soc. Am. B.* 6, 1221 (1989); Kiess, T. E., Shih, Y. H., Sergienko, A. V., and Alley, C. O., *Phys. Rev. Lett.* 71, 3893 (1993); Shih, Y. H. and Sergienko, A. V., *Phys. Lett. A* 186, 29 (1994); Sergienko, A. V., Shih, Y. H., and Rubin, M. H., *J. Opt. Soc. Am. B* 12, 859 (1995).
28. Atatüre, M., Di Giuseppe, G., Shaw, M. D., Sergienko, A. V., Saleh, B. E. A., and Teich, M. C., Phys. Rev. A 65, in press (2002) [eprint: http://xxx.lanl.gov/abs/quant-ph/0110154].
29. Atatüre, M., Di Giuseppe, G., Shaw, M. D., Sergienko, A. V., Saleh, B. E. A., and Teich, M. C., submitted to Phys. Rev. A (2001) [eprint: http://xxx.lanl.gov/abs/quant-ph/0111024].
30. Hong, C. K., Ou, Z. Y., and Mandel, L., *Phys. Rev. Lett.* 59, 2044 (1987); Kwiat, P. G., Steinberg, A. M., and Chiao, R. Y., *Phys. Rev. A* 47, R2472 (1993).
31. Rarity, J. G. and Tapster, P. R., *Phys. Rev. Lett.* 64, 2495 (1990).
32. Ou, Z. Y. and Mandel, L., *Phys. Rev. Lett.* 61, 50 (1988); Shih, Y. H. and Alley, C. O., *Phys. Rev. Lett.* 61, 2921 (1988); Shih, Y. H. and Sergienko, A. V., *Phys. Lett. A* 191, 201 (1994); Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V., and Shih, Y. H., *Phys. Rev. Lett.* 75, 4337 (1995).
33. Saleh, B. E. A., Abouraddy, A. F., Sergienko, A. V., and Teich, M. C., *Phys. Rev. A* 62, 043816 (2000).
34. Abouraddy, A. F., Saleh, B. E. A., Sergienko, A. V., and Teich, M. C., *J. Opt. Soc. Am. B* **in press** (February 2002).
35. Dauler, E., Jaeger, G., Muller, A., Migdall, A. L., and Sergienko, A. V., *J. Res. NIST* 104, 1 (1999).