PHYSICAL REVIEW A VOLUME 60, NUMBER 4 OCTOBER 1999

Quantum cryptography using femtosecond-pulsed parametric down-conversion

A. V. Sergienko,[1] M. Atatüre,[2] Z. Walton,[1] G. Jaeger,[1,3] B. E. A. Saleh,[1] and M. C. Teich[1,2]
[1]*Quantum Imaging Laboratory, Department of Electrical and Computer Engineering, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215*
[2]*Department of Physics, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215*
[3]*Starlab NV, Excelsiorlaan 40-42, B-1930 Zaventem, Belgium*
(Received 7 May 1999)

A new scheme for quantum cryptography, based on a distributed polarization quantum intensity interferometer, is presented. Two-photon entangled states generated via the optical nonlinear process of type-II phase-matched spontaneous parametric down-conversion are used to securely distribute secret cryptographic keys. The high contrast and stability of the quantum interference pattern obtained by using this design renders it superior to the best existing single-photon polarization technique. In addition, the use of high-repetition-rate femtosecond pump pulses for down-conversion significantly enhances the production rate of entangled photon pairs for key distribution. [S1050-2947(99)50910-4]

PACS number(s): 03.67.Dd, 42.50.Dv, 42.65.Ky

I. INTRODUCTION

Recent developments pertaining to the experimental investigation of fundamental problems of quantum mechanics have introduced a methodology for secure communications: quantum cryptography. At the heart of this technique lies the distribution of a cryptographic key whose security is guaranteed by the principles of quantum mechanics; attempts by an eavesdropper to read a quantum key affect the state in a readily detectable manner so that any insecure portions of a putative key can be immediately discarded and replaced by uninfluenced quantum bits, ensuring the security of the secret key.

In the past, quantum cryptography has had two principal implementations, both utilizing the quantum nature of the photon. One approach makes use of nearly single-photon states prepared from light initially in a coherent state obtained directly from the output of a laser [1,2]. This method suffers from the drawback that statistical fluctuations in the number of photons in such a coherent state allow for the occasional simultaneous presence of two or more photons in a single channel, and the transmitted photons go unmeasured before entering the communication channel. This, in turn, allows an eavesdropper to use one of these photons to extract information about the quantum key being distributed. The second approach [3] makes use of the nonlocal character of two-photon entangled [Einstein-Podolsky-Rosen (EPR)] [4] states generated indirectly from laser light by the nonlinear optical process of spontaneous parametric down-conversion (SPDC) [5]. The strong correlation of photon pairs, which are multiply entangled in energy-time and momentum-space, eliminates the problem of excess photons faced by the first approach. In the weak coherent-state approach, the exact number of photons actually injected is uncertain so that the channel is rendered insecure, whereas in the entangled-photon technique one of the pair of entangled photons is measured by the sender, confirming for the sender that the state is the appropriate one. However, the entangled-photon technique has in the past been implemented in a type-I configuration and has suffered from other limitations. These include low visibility and poor stability of the intensity interferometer and the concomitant need for the synchronous manipulation of interferometers well separated in space.

We have previously experimentally demonstrated that the use of doubly entangled EPR states generated by type-II SPDC [6] provides an enlarged realm of behavior and improved interference characteristics in comparison with type-I SPDC. In this paper, we demonstrate that a more flexible and robust method of quantum secure key distribution can be implemented using type-II SPDC in an improved configuration. Indeed, the high contrast and stability of the fourth-order quantum interference demonstrated by our design, along with the available knowledge of the exact number of photons present in the quantum communication channel, makes the performance of EPR-state-based quantum key distribution superior to the coherent-state-based technique.

II. ENTANGLED PHOTONS CREATED BY SPONTANEOUS PARAMETRIC DOWN-CONVERSION

An entangled-photon pair comprises a quantum state that cannot be written as a product of the quantum states of the individual photons. Investigations of fundamental quantum mechanics, such as probing the Einstein-Podolsky-Rosen paradox and the testing of the Bell inequalities [7], have centered on the correlations of particle properties inherent in these states. In particular, correlated photon pairs (biphotons) created via the nonlinear process of SPDC have permitted such investigations [1].

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 entangled photons. Entanglement in energy-time (or, equivalently, momentum-space) can thereby arise from the corresponding phase-matching, i.e., energy and momentum conservation:

$$\omega_1+\omega_2=\omega_p\,, \quad \vec{k}_1+\vec{k}_2=\vec{k}_p\,, \tag{1}$$

where ω_i is the frequency and $\vec{k}_i$ the wave vector, linking the

 ©1999 The American Physical Society

input pump (p) and output photons (1 and 2). The phase matching in down-conversion is type-I or type-II, depending on whether the photons in the pair have parallel or orthogonal polarizations, respectively. In addition, each of the photons of a pair that emerges from the nonlinear crystal may propagate in a different direction or they may propagate collinearly. The frequency and propagation directions of down-converted photons are determined by the orientation of the nonlinear crystal involved and the phase-matching relations that are satisfied.

For type-II collinear phase matching, the dispersion of the ordinary (o) and extraordinary (e) waves in a nonlinear crystal lead to a wave function Ψ whose space-time structure governs the relative positions of these two photons:

$$|\Psi\rangle = \int d\omega_1 \delta(\omega_1+\omega_2-\omega_p)\Psi(k_1+k_2-k_p)a_o^\dagger[\omega_1(k_1)]a_e^\dagger[\omega_2(k_2)]|0\rangle. \quad (2)$$

Here $a_o^\dagger$ and $a_e^\dagger$ are the creation operators for the ordinary and the extraordinary photons that comprise the pair.

III. QUANTUM KEY DISTRIBUTION WITH POLARIZATION-ENTANGLED PHOTONS

The visibility of an interference pattern is usually the central element of any scheme for quantum key distribution. Using two interferometers that are well separated in space, and synchronously varying the optical delays within and hence between them, EPR-pair nonlocal quantum correlations can be observed.

Only an undisturbed EPR state can produce 100% visibility. The intervention of any classical measurement apparatus (that is, eavesdropping) will cause an immediate reduction of the visibility to 70.7%. It is clear, therefore, that high visibility is required to ensure key security. Previous attempts to demonstrate the feasibility of quantum key distribution using EPR photons have not been inordinately successful because the required synchronous manipulation of two spatially separated Mach-Zehnder interferometers has hindered the observation of high visibility coincidences. To demonstrate that the EPR state can be a reliable tool for quantum cryptography, we have designed a new double, strongly unbalanced, distributed polarization intensity interferometer in which such simultaneous spatial manipulation is unnecessary. This provided much higher visibility and stability than any earlier attempt.

The scheme is illustrated in Fig. 1. A frequency-doubled femtosecond Ti:sapphire laser generates 80-fsec pulses at $\lambda_p = 415$ nm that are sent through a 0.1-mm-thick BBO crystal oriented so as to yield collinearly propagating degenerate down-converted photon pairs in accordance with the type-II phase-matching conditions imposed by the nonlinear crystal. We then manipulate the phase and position of the emitted photon pairs as follows. The photons enter two spatially separated interferometer arms via a polarization-insensitive 50/50 beam splitter (BS), which allows photons of both ordinary and extraordinary polarization to be reflected and transmitted with equal probability. One output port leads to a controllable polarization-dependent optical delay (the e-ray/o-ray loop) and thence to detector 1. The other leads, through an optical channel, to detector 2. Polarization analyzers are placed in front of each photon-counting detector and are oriented at 45° or −45°. This completes the creation of the polarization interferometer. Correlations are then registered by detecting the coincidence counts between the two detectors as a function of the optical delay between the orthogonally polarized photons. In this quantum key-distribution arrangement, the first beam splitter is located with the quantum key sender (Alice), while one of the output beam splitters is located at a distance with the receiver (Bob), as is evident in Fig. 1.

The resulting experimental polarization intensity interferogram is shown in Fig. 2. Each quantum bit (qubit) sent corresponds to one joint detection while the joint-detection rate provides a continuous security check. The interference pattern has two principal features. First, the full width at half-maximum of the interferogram envelope, arising when the e-ray/o-ray optical delay is varied, defines the entanglement time

$$T_e = \left(\frac{1}{v_o} - \frac{1}{v_e}\right)L. \quad (3)$$

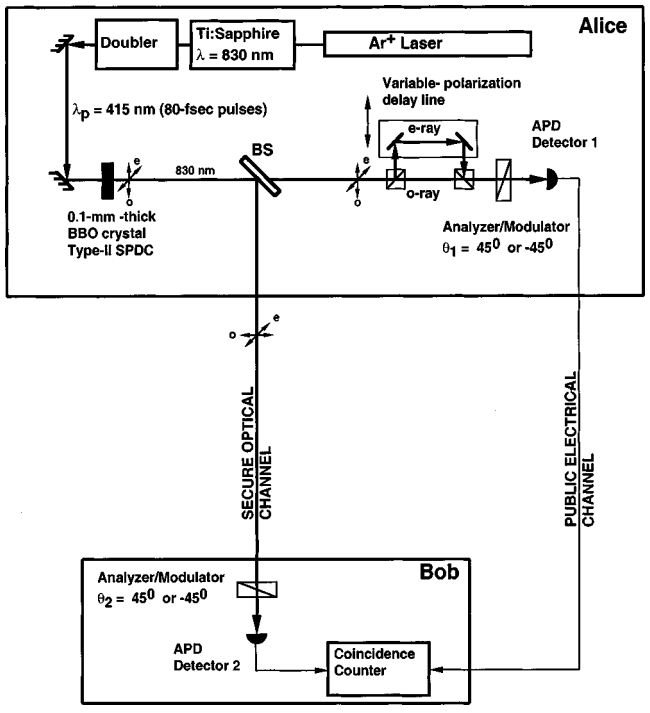

FIG. 1. Experimental arrangement for quantum cryptography using collinear type-II phase-matched entangled photons. The sender (Alice) is represented in the upper portion of the schematic whereas the receiver (Bob) occupies the lower portion.

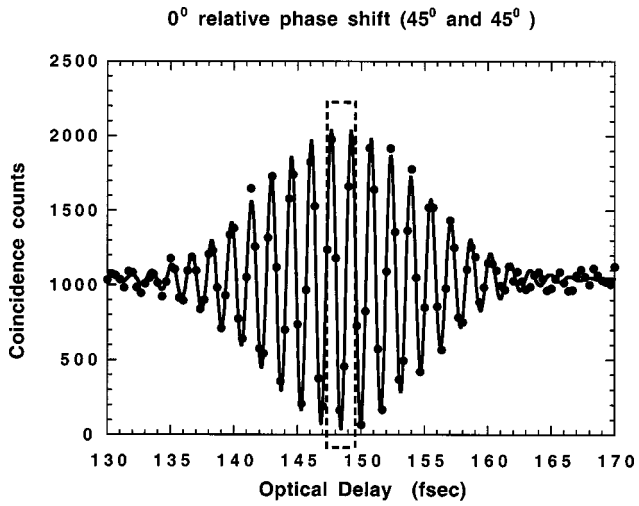

FIG. 2. Polarization intensity interferogram observed using a 0.1-mm-thick BBO crystal for down-conversion. The coincidence-time window is 3 nsec and the integration time for collecting the coincidence counts is 60 sec. The analyzers are set at $\theta_1 = 45°$ and $\theta_2 = 45°$ (0° relative phase shift). The *e*-ray/*o*-ray optical path delay is varied. Destructive interference at the central fringe corresponds to a ''0'' qubit being sent.

Here v_o and v_e are the group velocities of the ordinary and extraordinary waves, respectively, and L is the length of the crystal. The high-frequency carrier that resides under the envelope reflects the period of the uv pump wavelength rather than that of individual waves, and arises from the nonlocal entanglement of the twin beams.

As is shown in Fig. 3, a 90° phase shift of one of the analyzers modifies the quantum interference pattern so that the central fringe is constructive rather than destructive. The contrast is very high (~98%), as is evident from Fig. 4. This demonstrates that cryptographic key qubits—one value corresponding to each of the two sorts of interference—can be sent with a high degree of fidelity using this apparatus. In contrast, using type-I phase-matched SPDC, the fourth-order quantum interference visibility observed in coincidence between detectors at the outputs of interferometers has reached only about 85% visibility [8].

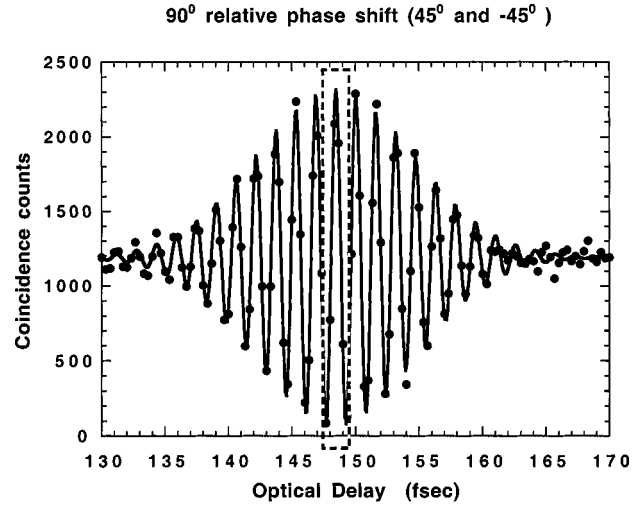

FIG. 3. The analyzers are set at $\theta_1 = 45°$ and $\theta_2 = -45°$ (90° relative phase shift). Constructive interference at the central fringe corresponds to a ''1'' qubit being sent.

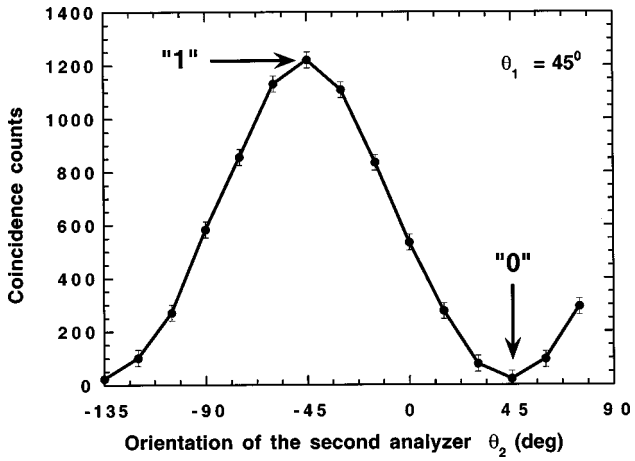

FIG. 4. Continuous transition from destructive to constructive interference at the central coincidence fringe observed by modulating the relative phase difference $\theta_2 - \theta_1$. The first polarizer is fixed at $\theta_1 = 45°$ while the angle θ_2 of the second analyzer is varied between $-135°$ and 90°. The integration time for collecting coincidence counts is 30 sec. The coincidence fringe contrast was ~98%.

The system operates as follows. The polarizations of the photons are randomly modulated by switching each analyzer-modulator in the rectilinear basis (45° and −45°), providing 0° or 90° relative phase shift between them. In order to complete the procedure of quantum-key distribution, it will also be necessary to randomly switch the polarization parameters of the two-photon entangled state between two nonorthogonal polarization bases, such as rectilinear and circular polarization. This can be accomplished using fast Pockels-cell polarization rotators. These sets of randomly selected angles force the mutual measurements by Alice and Bob to be destructive (a binary ''0'') or constructive (a binary ''1'') with a 50%-50% probability, depending on the mutual orientation of the modulators on both sides. Communications between Alice and Bob, which disclose the set of polarizer orientations selected during each measurement but not the measurement outcomes themselves, are then sent over a public electrical communication channel. Other protocols may be devised to endow this configuration with the full security that has been added to other configurations [9,10].

Furthermore, the use of high-repetition-rate femtosecond pump pulses significantly enhances the flux of entangled-photon pairs available for reliable and secure cryptographic key distribution. The down-converted photon pairs appear only at those well-defined times when pump pulses are present. A fixed 12.5-nsec timing separation between the pump pulses significantly enhances the performance of single-photon detectors, further increasing the high-fidelity detection rate. It is also noteworthy that the femtosecond timing of the key distribution significantly improves the scheme's potential for daylight operation.

IV. CONCLUSION

We have demonstrated that the phase-sensitive quantum interference of biphotons in a specially designed, strongly unbalanced, polarization intensity interferometer can be used to successfully implement secure quantum key distribution.

The high contrast and stability of the quantum interference demonstrated in this experiment have permitted us to finesse the specific limitations, and surpass the performance, of the best single-photon polarization techniques.

The impossibility of cloning a quantum state, and thus of extracting information from a quantum key without affecting it, is the basis of quantum cryptography. This entails a limitation on the distance of secure information transfer, namely the distance that the state can travel without absorption. The level of signal attenuation in modern fibers suggests a limit of 30–50 km for reliable quantum key distribution. Open-air communication, which is mandatory when fiber channels are unavailable, promises to be more feasible over large distances. We therefore plan to concentrate on the development of an open-air implementation of quantum cryptography.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation and by the Boston University Photonics Center.

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptology **5**, 3 (1992); J. D. Franson and H. Ilves, J. Mod. Opt. **41**, 2391 (1994); A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinder, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

[2] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luter, G. L. Morgan, and M. Schauer, Contemp. Phys. **36**, 149 (1995).

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

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

[5] Z. Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988); Y. H. Shih and C. O. Alley, *ibid.* **61**, 2921 (1988); P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **47**, 2472 (1993); J. Brendel, E. Mohler, and W. Martienssen, Phys. Rev. Lett. **66**, 1142 (1991); T. S. Larchuk, R. A. Campos, J. G. Rarity, P. R. Tapster, E. Jakeman, B. E. A. Saleh, and M. C. Teich, *ibid.* **70**, 1603 (1993); T. E. Kiess, Y. H. Shih, A. V. Sergienko, and C. O. Alley, *ibid.* **71**, 3893 (1993).

[6] M. H. Rubin, D. N. Klyshko, Y. H. Shih, and A. V. Sergienko, Phys. Rev. A **50**, 5122 (1994); P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. H. Shih, Phys. Rev. Lett. **75**, 4337 (1995).

[7] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).

[8] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); A. K. Ekert and G. M. Palma, J. Mod. Opt. **41**, 3413 (1994); J. G. Rarity and P. R. Tapster, Phys. Rev. A **45**, 2052 (1992).

[9] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984 (IEEE, New York, 1984), p. 175.

[10] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992), and references therein.