QUANTUM CRYPTOGRAPHY WITH FEMTOSECOND PARAMETRIC DOWN CONVERSION

A. V. Sergienko, M. Atature, B. M. Jost, J. Perina Jr., B. E. A. Saleh, and M. C. Teich

Quantum Imaging Laboratory
Department of Electrical and Computer Engineering
Boston University
Boston MA 02215

Abstract

We experimentally demonstrate a quantum cryptography system using two-photon entangled (EPR) states generated via the nonlinear process of spontaneous parametric down conversion pumped by a femtosecond laser. There are two major approaches in quantum cryptography which historically appeared almost simultaneously. One uses the quantum features of single photon states produced by significant attenuation of original light in a coherent state. The other is based on the quantum nonlocal character of two-photon entangled EPR states. The applicability of the latter one was strongly limited because of low visibility and poor stability of the systems which require synchronous manipulation of two Mach-Zehnder interferometers well separated in space. We developed a new scheme for quantum cryptography which is based on the use of a distributed polarization quantum intensity interferometer. This technique utilizes a double-entangled EPR quantum states generated in the nonlinear process of type-II spontaneous parametric down conversion (SPDC). The high contrast and stability of quantum interference demonstrated in our preliminary experiments promises to bring the performance of this system above the level of the best single-photon polarization techniques, and to do so without their specific limitations. The use of a high-repetition rate femtosecond pulses as a pump source enhances significantly the flux of entangled photon pairs available for the reliable and secure key distribution.

INTRODUCTION

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. Recent developments in experimental tests of the fundamental problems of quantum mechanics, such as the Einstein-Podolsky-Rosen (EPR) paradox and the violation of Bell's inequalities, [1] 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 has made use of two principal approaches that utilize the quantum nature of the photon state. One approach makes use of near single-photon states prepared from light initially in a coherent state [2, 3]. Its major drawback arises from the statistical fluctuations of the number of photons in the original state. This adds the possibility of simultaneously having two photons in the channel; the eavesdropper can use the second one to extract partial information. The other approach is based on the nonlocal character of two-photon entangled (EPR) states generated in the nonlinear optical process of spontaneous parametric down conversion (SPDC) [4, 5]. The unique correlation of two photons in space, time, energy, and momentum resolves the problem inherent in the first approach. Unfortunately, the applicability of the latter technique has been severely limited because of low visibility and poor system stability inherent in the use of type-I SPDC, as well as the need for the synchronous manipulation of two Mach-Zehnder interferometers that are well separated in space.

Based on our previous experimental results [1], we have demonstrated that the use of doubly entangled EPR states generated by type-II SPDC provides richer physics then type-I SPDC, and thereby creates a more flexible, robust, and reliable quantum apparatus for cryptographic appliacations. 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 beyond the level of the best single-photon systems.

The key feature of quantum cryptography, that is, the impossibility of cloning the quantum state or extracting information without destroying it, carries with it a major limitation on the distance of secure information transfer. The limit is the distance that a single-photon state can travel without absorption. The level of signal attenuation in modern fibers would appear to pose a limit of 30-50 km for reliable quantum cryptography. 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 a vital issue in modern telecommunications. 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 is expected to become a crucial tool in these situations. The thickness of the atmospheric layer is several kilometers and its density rapidly decreases with altitude, making ground-to-satellite communication attractive. Satellite-to-satellite communications using our cryptographic method, in the vacuum of open space, has only one problem — how to collimate and point the beam. Finally, the synthesis of both approaches - local distribution over fiber lines and transmittion over the horizon using a

satellite-based link, can provide a global secure communication network (see Fig.1).

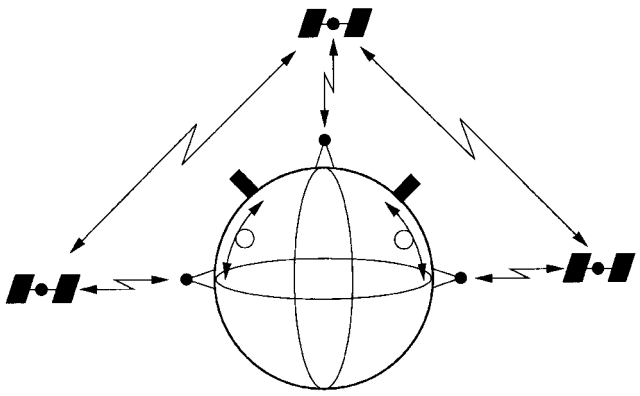

Figure 1. Illustration of combined short-distance optical fiber and long-distance open-air secure communication.

Entangled Photons Created by Spontaneous Parametric Downconversion

Correlated (entangled) two-particle states have been known since the early 1920's. Entangled states comprise two or more particles whose state cannot be written as products of single-particle states [6]. These states have played an important role in the study of the basic questions of quantum mechanics such as the Einstein-Podolsky-Rosen (EPR) paradox [7] and tests of Bell's inequalities [8]. Two-photon correlations of the light created in the nonlinear process of SPDC permit the investigation of many fundamental issues of quantum mechanics of photons [1]. 3

In spontaneous parametric down conversion, a pump laser beam is incident on a birefringent crystal. Nonlinear effects in the crystal lead to the spontaneous emission of pairs of entangled light quanta. The entanglement in frequency-wavenumber space, or equivalently space-time, comes from the frequency- and phase-matching (equivalently energy- and momemtum-conserving) conditions [9, 10, 11]

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

where ω_i is the frequency and $\mathbf{k}_i$ the wave number, linking the input pump (p), and output signal (1) and idler (2). The down conversion is called Type-I or Type-II depending on whether the photons in the pair have parallel or orthogonal polarizations. The photon pair that emerges from the nonlinear crystal 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. Initially, Type-I SPDC was used extensively as a convenient source of two-photon entangled states [1].

It was shown recently in our work that Type-II SPDC provides a richer tool due to the two-photon entanglement both in space-time and in polarization (spin) [12]. The

dispersion of the ordinary and extraordinary waves in a nonlinear crystal lead 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 positions of these two photons in space-time.

Experimental attempts to develop quantum cryptography using Type-I entangled-photon pairs (EPR states) was initiated shortly after the notion was introduced by Ekert [4]. This approach requires the use of a Franson-type interferometer [13]. 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 lead to an almost 100% visibility of quantum interference observed in coincidence between detectors at the output of each interferometer.

The visibility is the most crucial parameter in this technique. Only undisturbed quantum state will produce $\sim 100\%$ visibility. Intervention of any classical measurement apparatus (eavesdropping) will cause an immediate reduction of visibility to 75% providing clear evidence of intrusion.

However, practical attempts to demonstrate the feasibility of quantum cryptography with EPR photons in fibers were not very successful. The applicability of the this technique has been severely limited because of low visibility inherent in the need of synchronous manipulation of the two spatially separated Mach-Zehnder interferometers.

CRYPTOGRAPHY WITH POLARIZED ENTANGLED PHOTONS

To demonstrate that the EPR state is a reliable tool for quantum cryptography we designed a new approach using non-local quantum interference of two-photon entangled states (EPR states) generated in Type-II SPDC. It is based on the use of a double, strongly unbalanced, and distributed polarization interferometer as shown in Fig.2.

Polarization-entangled photons are created by sending frequency doubled femtosecond Ti:Sapphire laser pulses through an appropriately oriented Type-II second-order nonlinear BBO crystal. Using the experimental system in Fig. 2, one can accurately manipulate the phase and position of the emitted entangled photon pairs. 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 degrees in front of each photon counting detector completes the creation of the polarization interferometer. Signal correlation is registered by detecting the coincidence counts between the two detectors as a function of the polarization delay.

The crucial features of this quantum interferometer are:

Double - One input beamsplitter (BS) and two output polarization beamsplitters (analyzers at 45°), well-separated in space.

Strongly unbalanced - polarization delay line introduced only in one interferometer.

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

Nonlocal 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 - Type-II SPDC and polarization analyzers at the output beamsplitter.

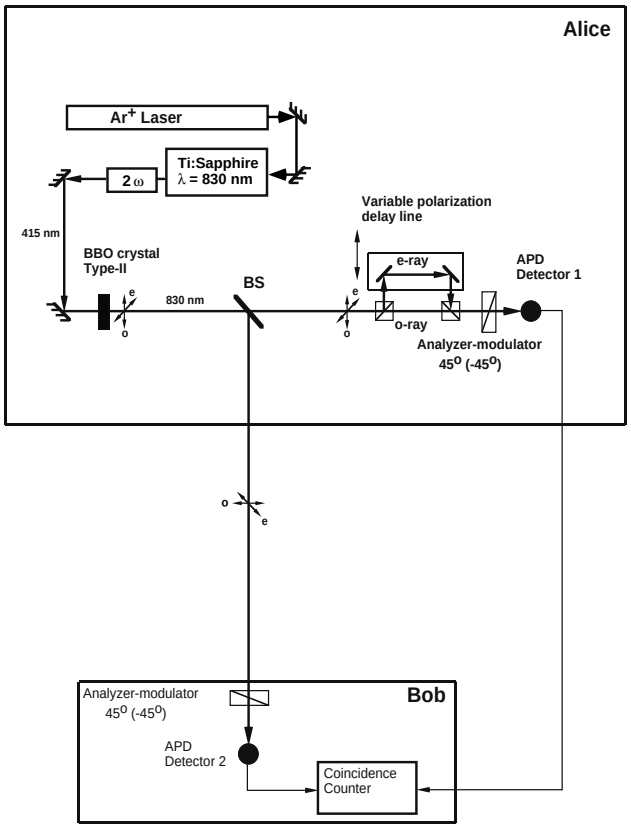

Figure 2. Schematic of the experimental setup for the generation of Type-II entangled photons (with orthogonal polarization) and their registration using quantum interference with coincidence detection.

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

Results obtained using this experiment are shown in Fig.3. The pattern in this figure arises from the contributions of two effects. First, the full-width at half-maximum of the envelope defines the coherence time

$$T_{coh} = \left(\frac{1}{u_o} - \frac{1}{u_e}\right) L_c \tag{2}$$

where u_o and u_e are the group velocities of the ordinary and extraordinary waves and L_c is the length of the crystal. Second, the internal modulation has a period that depends only on the pump wavelength.

The 90° shift of the phase in one of the analyzers will change the quantum interference immediately so as to be constructive (rather than destructive) at the central fringe (see Fig.5) with a very high ($\sim 99\%$) contrast.

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 fast Pockels-cell polarization rotators in front of the detectors .

These two sets of selected angles will force the mutual measurement by Alice and Bob to be a binary "0" (destructive) or "1" (constructive) with 50%-50% probability.

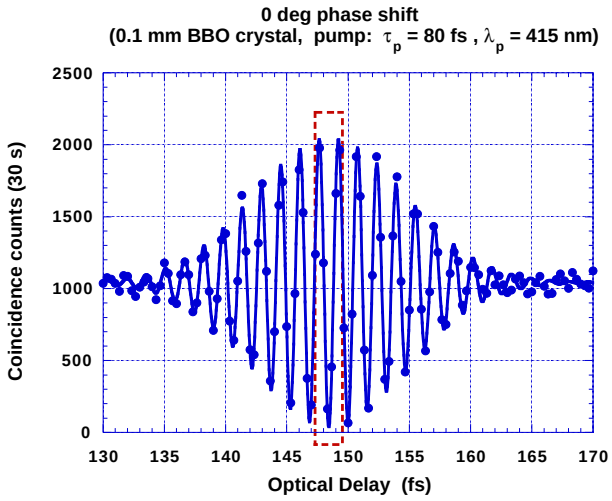

Figure 3. Experimentally obtained intensity correlation function from a 0.1-mm thick BBO crystal. The high-frequency carrier inside the envelope reflects the period of the UV pump wavelength rather than of inividual signal or idler waves. This is due to the two-photon entanglement of the twin beams. This quantum *destructive* interference is observed at **0 deg phase shift** between polarization analyzers.

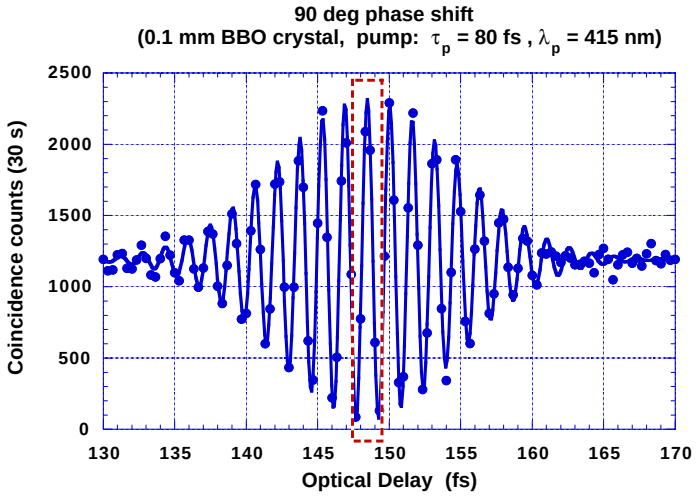

Figure 4. Experimentally observed *constructive* interference at **90 deg phase shift** between polarization analyzers.

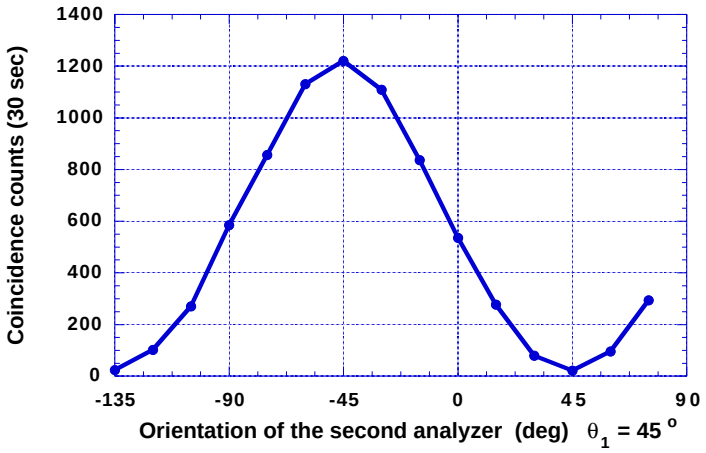

Figure 5. Experimentally observed modulation at the central fringe as a function of relative position of polarization modulators. 99% visibility insures a strong violation of Bell's inequalities.

Each particular outcome depends on mutual orientation of modulators on both sides. Discussion between Alice and Bob over the public public communication channel of which set of orientations was selected in each trial but not what was the outcome will complete the standard quantum key distribution described in a literature [4, 14, 15].

The use of high-repetition rate femtosecond pulses as a pump source enhances significantly the flux of entangled photon pairs available for reliable and secure key distribution. The downconverted entangled pairs appear only at well-defined times when pump pulses are present. A fixed 12.5-ns timing separation between the pump pulses enhances significantly the performance of single-photon detectors increasing the high-fidelity detection rate. The femtosecond timing will help significantly to develop a daylight operating communication system.

Our study has shown that the phase-sensitive quantum interference of two entangled photons in a 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 preliminary experiments promises to bring the performance of this system above the level of the best single-photon polarization techniques, and to do so without their specific limitations.

REFERENCES

1. Ou, Z. Y. and Mandel, L., *Phys. Rev. Lett.* 1988, 61:50; Shih, Y. H. and Alley, C. O., 1988, *Phys. Rev. Lett.* 61:2921; Hong, C. K., Ou, Z. Y., and Mandel, L., *Phys. Rev. Lett.* 1987, 59:2044; Ou, Z. Y. and Mandel, L., *Phys. Rev. Lett.* 1988, 61:54; Kwiat, P. G., Steinberg, A. M., and Chiao, R. Y., *Phys. Rev. A.*, 1993, 47:2472; Brendel,J., Mohler, E., and Martienssen, W.,*Phys. Rev. Lett.* 1991, 66:1142; 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.* 1993, 70:1603; Steinberg, A. M., Kwiat, P. G., and Chiao, R. Y., *Phys. Rev. Lett.* 1993, 71:708; Hong, C. K., Ou, Z. Y., and

Mandel, L., *Phys. Rev. Lett.* 1987, 59:1903; Rarity, J. G., and Tapster, P. R.,*J. Opt. Soc. Am. B.* 1989, 6:1221; Kiess, T. E., Shih, Y. H., Sergienko, A. V., and Alley, C. O., *Phys. Rev. Lett.* 1993, 71:3893; Shih, Y. H. and Sergienko, A. V., *Phys.Lett A.* 1994, 186:29; Sergienko, A. V., Shih, Y. H., and Rubin,M. H., *J. Opt. Soc. Am. B.* 1995, 12:859.

2. Bennett, C. H., Bessette, F., Brassard, G., Savail, L., and Smolin, J., *Journal of Cryptology.* 1992, 5:3; Bennett, C. H., Brassard, G., Mermin, N. D, *Phys. Rev. Lett.* 1992, 68:557; Bennett, C H., Wiesner, S. J., *Phys. Rev. Lett.* 1992, 69:2881; Breguet, J., Muller, A., and Gisin, N., *Journal of Mod. Opt.* 1994, 41:2405, Franson, J. D. and Ilves, H., *J. of Mod. Opt.* 1994, 41:2391; Franson, J. D. and Jacobs, B. C., *Electronic Letters* 1995, 31:232; Muller, A., Herzog, T., Huttber, B., Tittel, W., Zbinder, H., and Gisin, N., *Appl. Phys. Lett.* 1997, 70:793.
3. Hughes, R. J., Alde, D. M., Dyer, P., Luter, G. G., Morgan, G. L., and Schauer, M., *Contemporary Physics* 1995, 36:149.
4. Ekert, A. K., *Phys. Rev. Lett.* 1991, 67:661; Ekert, A. K., and Palma, G. M., *J. of Mod. Opt.* 1994, 41:3413; Rarity, J. G., Owens, P. C. M., and Tapster, P. R., *J. of Mod. Opt.* 1994, 41:2435; Rarity, J. G., and Tapster, P. R., *Phys. Rev. A.* 1992, 45:2052.
5. Ekert, A. K., Palma, G. M., Rarity, J. G., and Tapster, P. R., *Phys. Rev. Lett.* 1992, 69:1293.
6. Schrödinger, E., *Naturwissenschaften* 1935, 23:807, [Translation *in* 1983, "Quantum Theory of Measurement," ed. Weeler, J. A., and Zurek, W. H., Princeton University Press Princeton].
7. Einstein, A., Podolsky, B., and Rosen, N., *Phys. Rev.* 1935, 47:777.
8. Bell, J. S., *Physics* 1964, 1:195.
9. Yariv, A., 1967, "Quantum Electronics," Wiley, New York.
10. Klyshko, D. N., 1988, "Photons and nonlinear optics," Gordon and Breach, New York.
11. Blombergen, N., 1965, "Nonlinear Optics," Benjamin, New York.
12. Rubin,M. H., Klyshko, D. N., Shih, Y. H., and Sergienko, A. V., *Phys.Rev. A.* 1994, 50:5122; Shih, Y. H., and Sergienko, A. V., *Phys.Rev. A.* 1994, 50:2564; Pittman, T. B., Sergienko, A. V., Shih, Y. H., and Rubin,M. H., *Phys.Rev. A.* 1995, 51:3495; Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V., and Shih, Y. H., *Phys. Rev. Lett.* 1995, 75:4337.
13. Franson, J. D., *Phys. Rev. Lett.* 1989, 62:2205.
14. Bennett, C. H., Brassard, G., 1984 *in* "Proc. Int. Conf. Computer Systems and Signal Processing," Bangalor, 175.
15. Bennett, C. H., *Phys. Rev. Lett.* 1992, 68:3121.