PHYSICAL REVIEW
LETTERS

VOLUME 69 31 AUGUST 1992 NUMBER 9

Practical Quantum Cryptography Based on Two-Photon Interferometry

Artur K. Ekert
Merton College & Physics Department, Oxford University, Oxford, OX1 4JD, United Kingdom

John G. Rarity and Paul R. Tapster
Defence Research Agency, Royal Signals and Radar Establishment, St. Andrews Rd., Malvern WR14 3PS, United Kingdom

G. Massimo Palma
C.N.R. Istituto per le Applicazioni Interdisciplinari della Fisica via Archirafi 36, I-90123 Palermo, Italy
(Received 30 March 1992)

We propose an experimental realization of a cryptographic-key-sharing scheme exploiting quantum correlations between pair photons. Our experimental setup consists of an external source of correlated photon pairs which propagate to two widely separated unbalanced Mach-Zehnder interferometers. The probability of detection of photon pairs in any two outputs of the interferometers can be fully modulated by phase plates in either interferometer.

PACS numbers: 03.65.Bz, 42.50.Wm, 89.70.+c

Quantum cryptography, a new branch of physics and cryptology, employs quantum phenomena such as the uncertainty principle and quantum correlations to protect distributions of cryptographic keys. Key distribution is defined as a procedure allowing two legitimate users of a communication channel to establish two exact copies, one copy for each user, of a random and secret sequence of bits. This random sequence, meaningless as such, is called *a key* and can subsequently be used as a basis for encrypting messages between the two users. The security of any further encrypted communication depends directly on the security of the key distribution.

Conventional cryptography provides no tools for provable security of the key distribution and any classical encoding is vulnerable to passive interception. Such interception may be difficult from the technological point of view but is perfectly allowed by the laws of classical physics and therefore the two legitimate users can never be sure that there exist only two and no more copies of the key.

In a simplistic way, any totally passive eavesdropping can be viewed as a two-stage process. The first stage amounts to making a copy of the carrier of information and the second to reading from the cloned copy (or copies) a set of values of observables that are used for the encoding of the key. The intercepted original carrier is sent over to the legitimate receiver, who is unable to check whether the carrier has been intercepted or not because the state of the carrier has not been altered during the cloning process. According to quantum theory the first stage of passive eavesdropping cannot in general be completed [1]. Quantum cloning will give a positive result leaving the state of the original intact only if the adversary knows in advance that the carrier of information is in a quantum state picked up from a particular set of orthonormal states. If this is not the case, the adversary will not be able to construct a cloning device; a device of this sort would effectively violate the uncertainty principle enabling measurements of noncommuting observables on different copies of the carrier. This shows that coding based, for example, on nonorthogonal states or quantum correlations which cannot be cloned gives a chance to avoid eavesdropping.

Quantum cryptography, which employs quantum mechanics to improve the security of communication, was originated by Bennett, Brassard, and Wiesner [2,3]. Theoretical models for quantum key distributions based on the uncertainty principle have been analyzed by Bennett and Brassard [3] and models based on quantum correlations have been proposed by Ekert [4]. The first practical implementation of the cryptosystem based on the uncertainty principle has been performed by Bennett,

Bessette, Brassard, Salvail, and Smolin [5]; here we describe a practical realization of a quantum channel which distributes the key and protects it against eavesdropping using the nature of quantum correlations.

A scheme of the apparatus is shown in Fig. 1. A parametric down-conversion source is pumped by a monochromatic short-wavelength laser of frequency $2\omega_0$ ($\lambda_0 = 441.6$ nm in the experiment). Signal and idler photons are emitted in a broadband cone behind the crystal with pairs satisfying energy and momentum conservation. Photon pairs are selected by placing apertures in the down-converted cone satisfying the phase-matching conditions in the crystal. Signal and idler photons are launched into separate fiber-optic cables and propagate to remote Mach-Zehnder interferometers. Each interferometer contains a shorter and a longer path with the difference in transit time over the two paths denoted by ΔT ($\Delta T \simeq 1$ ns in the experiment). Signal photon detectors labeled S_1 and S_0 and idler detectors labeled I_1 and I_0 view the four Mach-Zehnder outputs.

This experimental setup has been analyzed in detail by Franson [6] and by Rarity and Tapster [7] in connection with Bell's inequalities. Here, we present a simplified but sufficient description of the nonlocal correlation phenomenon that can be observed in this system.

We assume that the output state is a two-photon entangled state of the signal and the idler, which we write as

$$|\Psi\rangle = \int d\omega\, c(\omega) |1;\omega\rangle \otimes |1;2\omega_0 - \omega\rangle , \tag{1}$$

where we can choose ω to denote the frequency of the signal photon ω_s, and consequently, due to energy conservation, the frequency of the idler photon ω_i can be written as $2\omega_0 - \omega$.

The function $|c(\omega)|^2$ is positive in the interval of the order $\Delta\omega$ centered at ω_0. The calculation of the joint probability of registering photons at time $t+dt$ by the signal and idler detectors amounts to summing the probability amplitudes for the photons to have traversed various paths to the detectors and taking the square modulus of the total probability amplitude. If we take into account that $1/\Delta\omega \ll \Delta T$ ($\Delta\lambda \simeq 3$ nm in the experiment), then after simple calculations we obtain

$$p(1,1) = p(0,0) = \tfrac{1}{4}[1 + \cos(\phi_s + \phi_i + \theta)] , \tag{2}$$

$$p(0,1) = p(1,0) = \tfrac{1}{4}[1 - \cos(\phi_s + \phi_i + \theta)] , \tag{3}$$

where the signal phase shift ϕ_s and idler phase shift ϕ_i can be set up independently in the respective interferometers, and $\theta = (\omega_s + \omega_i)\Delta T = 2\omega_0 \Delta T$. In our notation $p(0,1)$ means that the signal photon has been registered by detector S_0 and the idler photon has been registered by detector I_1 within the small time interval $dt \ll \Delta T$. The coefficient of correlation, assuming perfect detection and fixing $\theta = 2k\pi$, $k = 1,2,3,\ldots$, is given by

$$J(\phi_s,\phi_i) = p(1,1) + p(0,0) - p(0,1) - p(1,0)$$
$$= \cos(\phi_s + \phi_i) . \tag{4}$$

The coefficient depends on the sum of two local parame-

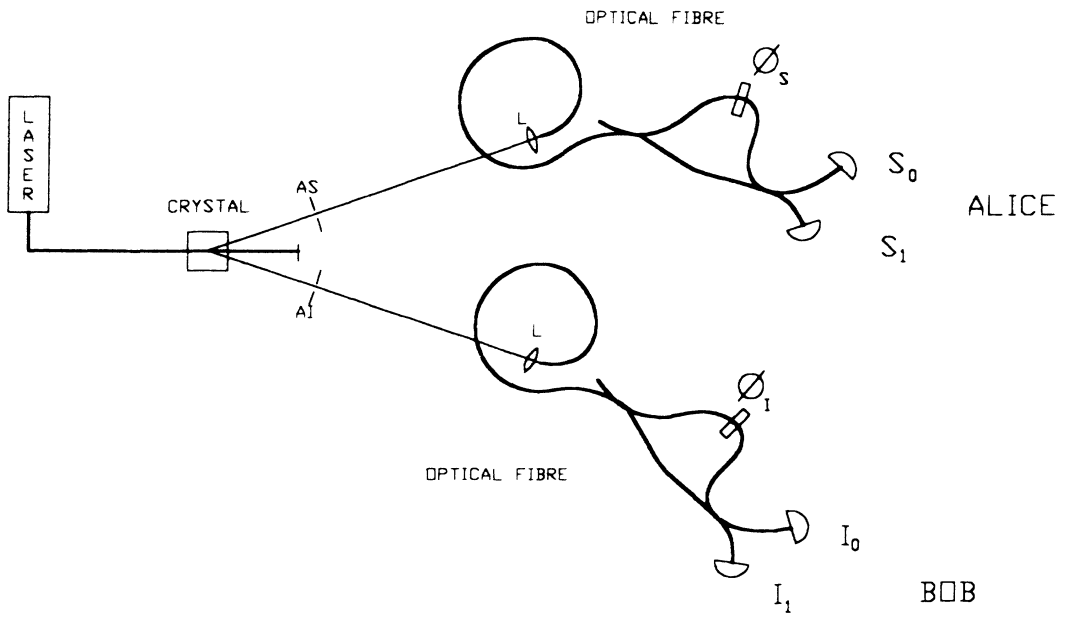

FIG. 1. Scheme of the quantum public key distribution apparatus. A short-wavelength laser illuminates a suitably cut nonlinear crystal. Apertures A_S and A_I select photon pair beams which are launched into single-mode fibers by lenses L. Identical Mach-Zehnder interferometers are placed in the signal and idler arms of the apparatus and interferometer outputs are viewed by signal S_0,S_1 and idler I_0,I_1 single-photon counting detectors. Alice and Bob view these outputs and confirm coincident (within dt) photon detections and relevant phase settings ϕ_s,ϕ_i via a separate public channel.

ters ϕ_s and ϕ_i, which results in a nonlocal character of correlation between the photocounts in the two distant interferometers. We note that for $\phi_s+\phi_i=0$ there is a perfect correlation between photocounts in the two distant interferometers. Let us now describe how this nonlocal quantum phenomenon can be used for key distribution.

Two legitimate users of the two distant interferometers, whom we traditionally call Alice and Bob, will set up the local parameters randomly and independently for each incoming photon. Alice, who receives the signal mode, will choose randomly between $\phi_s=0$ and $\phi_s=\pi/2$, and Bob, who receives the idler mode, will choose randomly between $\phi_i=0$ and $\phi_i=-\pi/2$. After transmission they reveal publicly the setting of their local parameters, but not which detector registered a photon. They then agree to discard all instances in which $\phi_s+\phi_i\neq 0$, as well as instances in which one or both detectors failed to register a photon due to imperfect quantum efficiency. The remaining instances ought to refer to perfectly correlated photocounts, $\phi_s+\phi_i=0$. To verify that this is so, Alice and Bob publicly compare the results of the photocounts on a sufficiently large random subset of the undiscarded instances. If they find that the tested subset is indeed perfectly correlated, they can infer that the remaining untested subset is also perfectly correlated, and therefore can form the cryptographic key. In a practical realization the test for eavesdropping must be more sophisticated than the subset test described above. A more useful test involves error-correction and hashing techniques [5,8].

Nonlocal interference effects of this type have been observed in short-range laboratory experiments with measured correlation coefficients J [Eq. (4)] up to 90% [9,10]. We have performed a preliminary experiment where one beam propagated over 170 m through a multimode optical fiber before the interferometer, but here the measured correlation coefficient was low, partly due to poor time resolution in the detectors [7]. Such an experiment could easily be improved by using single-mode fiber and in-line fiber interferometers (Fig. 1). To ensure high visibility the detector resolution dt must be smaller than the time difference between the long and short paths, ΔT, to discriminate against noninterfering events. In an all fiber apparatus, dispersion effects in the out-of-balance interferometers can be avoided by reduction of bandwidth and operation close to the dispersion minimum (1.3 μm in conventional fibers). This choice also has the advantage of low loss but requires further development of suitable photon counting detectors [11]. With careful control of the apparatus, correlation coefficients greater than $J=0.95$ should routinely be achieved. This implies a high-bit error rate of 5×10^{-2}. This can be substantially reduced without compromising security using suitable error-correction procedures [8]. The range of a realistic system will depend on losses, which in communication fibers can be as low as 0.17 dB/km, coupled with the minimum acceptable data rate. Recent free-space communication experiments have demonstrated that propagation losses of some 20 dB or more could be tolerated [12].

The analysis of the security of this system is equivalent to the analysis of the security for the EPR-type cryptosystems provided by Ekert [4] and Bennett, Brassard, and Mermin [13]. The advantage of this system over these previous schemes is that it uses interference rather than polarization phenomena. Maintaining polarization in optical fiber (without in effect measuring it) is not possible using present technology. Using standard low-loss, low-dispersion communication fiber and polarization-insensitive interferometers our system may be capable of key sharing over long ($\sim$10–20 km) distances.

One of us (G.M.P.) acknowledges partial financial support from the Italian INFM and GNSM. He would like also to thank Dr. Keith Burnett for his kind hospitality at Clarendon Laboratory where part of this work has been done.

Note added.—After we submitted the paper we learned about the new, non-EPR interferometric key distribution scheme proposed recently by Bennett [14]. Bennett's system will increase the key distribution range to a level comparable with our estimated range. As yet, there is insufficient ground to conclude which of the schemes is more practical.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] S. Wiesner, Sigact News **15** (1), 78 (1983).
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[6] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989); **67**, 290 (1991).
[7] J. G. Rarity and P. R. Tapster, Phys. Rev. A **45**, 2052 (1992).
[8] C. H. Bennett, G. Brassard, and J-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[9] J. G. Rarity and P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990); see also J. G. Rarity, P. R. Tapster, E. Jakeman, T. Larchuk, R. A. Campos, M. C. Teich, and B. E. A. Saleh, Phys. Rev. Lett. **65**, 1384 (1990).
[10] J. Brendel, E. Mohler, and W. Martienssen, Phys. Rev. Lett. **66**, 1142 (1991).
[11] B. F. Levine and C. G. Bethea, Appl. Phys. Lett. **44**, 553 (1984).
[12] S. F. Seward, P. R. Tapster, J. G. Walker, and J. G. Rarity, Quantum Opt. **3**, 201 (1991).
[13] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[14] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).