Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol

D. S. Naik,[1] C. G. Peterson,[1] A. G. White,[1,2] A. J. Berglund,[1] and P. G. Kwiat[1,*]

[1]*Physics Division, P-23, Los Alamos National Laboratory, Los Alamos, New Mexico 87545*

[2]*Department of Physics, University of Queensland, Brisbane, Queensland 4072, Australia*

(Received 18 October 1999)

Using polarization-entangled photons from spontaneous parametric down-conversion, we have implemented Ekert's quantum cryptography protocol. The near-perfect correlations of the photons allow the sharing of a secret key between two parties. The presence of an eavesdropper is continually checked by measuring Bell's inequalities. We investigated several possible eavesdropper strategies, including pseudo–quantum-nondemolition measurements. In all cases, the eavesdropper's presence was readily apparent. We discuss a procedure to increase her detectability.

PACS numbers: 03.67.Dd, 03.65.Bz, 42.79.Sz

The emerging field of quantum information science aims to use the nonclassical features of quantum systems to achieve performance in communications and computation that is superior to that achievable with systems based solely on classical physics. For example, current methods of public-key cryptography base their security on the supposed (but unproven) computational difficulty in solving certain problems, e.g., finding the prime factors of large numbers—these problems have not only been unproven to be difficult, but have actually been shown to be computationally "easy" in the context of quantum computation [1]. In contrast, it is now generally accepted that techniques of quantum cryptography can allow completely secure communications between distant parties [2–5]. Specifically, by using single photons to distribute a secret random cryptographic key, one can ensure that no eavesdropping goes unnoticed; more precisely, one can set rigid upper bounds on the possible information known to a potential eavesdropper, based on measured error rates, and then use appropriate methods of "privacy amplification" to reduce this information to an acceptable level [6].

Since its discovery, quantum cryptography has been demonstrated by a number of groups using weak coherent states, both in fiber-based systems [7] and in free space arrangements [8,9]. These experiments are provably secure against all eavesdropping attacks based on presently available technology; however, there are certain conceivable attacks to which they are might be vulnerable, as sometimes the pulses used necessarily contain more than one photon—an eavesdropper could in principle use these events to gain information about the key without introducing any extra errors [10]. Use of true single-photon sources can close this potential security loophole; and while the loophole still exists when using *pairs* of photons as from parametric down-conversion (because occasionally there will be *double* pairs), it has been shown that they may allow secure transmissions over longer distances [11].

While a number of groups use correlated photon pairs to study nonlocal correlations (via tests of Bell's inequalities [12–14]), and their possible application for quantum cryptography [15,16], to our knowledge no results explicitly using entangled photons in a quantum cryptographic protocol have been reported in the literature [17]. It is now well established that one cannot employ these nonlocal correlations for superluminal signaling [18]. Nevertheless, Ekert showed that one can use the correlations to establish a secret random key between two parties, as part of a completely secure cryptography protocol [3].

In our version of the Ekert protocol, "Alice" and "Bob" each receive one photon of a polarization-entangled pair in the state $|\phi^+\rangle = (|H_1H_2\rangle + |V_1V_2\rangle)/\sqrt{2}$, where H (V) represents horizontal (vertical) polarization. They each, respectively, measure the polarization of their photons in the bases $(|H_1\rangle + e^{i\alpha}|V_1\rangle)$ and $(|H_2\rangle + e^{i\beta}|V_2\rangle)$, where α and β randomly take on the values $\alpha_1 = 45°$, $\alpha_2 = 90°$, $\alpha_3 = 135°$, $\alpha_4 = 180°$; $\beta_1 = 0°$, $\beta_2 = 45°$, $\beta_3 = 90°$, $\beta_4 = 135°$. They then disclose by public discussion which bases were used, but not the measurement results. For the state $|\phi^+\rangle$, the probabilities for a coincidence between Alice's detector 1 (or detector $1'$, which detects the orthogonally polarized photons) and Bob's detector 2 ($2'$) are given by

$$\begin{aligned} P_{12}(\alpha,\beta) &= P_{1'2'}(\alpha,\beta) = [1 + \cos(\alpha + \beta)]/4\,, \\ P_{12'}(\alpha,\beta) &= P_{1'2}(\alpha,\beta) = [1 - \cos(\alpha + \beta)]/4\,. \end{aligned} \tag{1}$$

Note that when $\alpha + \beta = 180°$, they will have completely correlated results, which then constitute the quantum cryptographic key. As indicated in Table I, the results from other combinations are revealed and used in two independent tests of Bell's inequalities, to check the presence of an intermediate eavesdropper ("Eve"). Here we present

TABLE I. Distribution of data dependent on Alice's and Bob's respective phase settings α_i and β_i (see text for details).

		Alice			
		α_1	α_2	α_3	α_4
Bob	β_1	S	$\cdots$	S	QKey
	β_2	$\cdots$	S'	QKey	S'
	β_3	S	QKey	S	$\cdots$
	β_4	QKey	S'	$\cdots$	S'

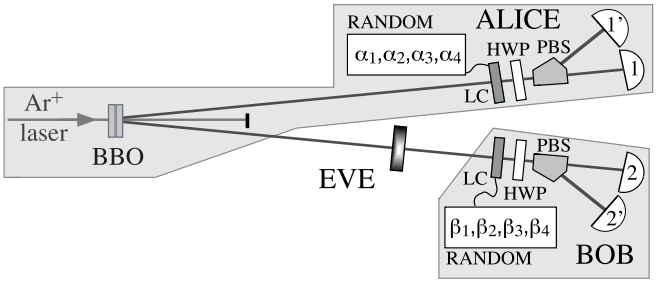

FIG. 1. Schematic of quantum cryptography system. 351.1 nm light from an Argon ion laser is used to pump two perpendicularly oriented nonlinear optical crystals (BBO). The resultant entangled photons are sent to Alice and Bob, who each analyze them in one of four randomly chosen bases. The eavesdropper, if present, was incorporated using either a polarizer or a decohering birefringent plate [both orientable, and in some cases with additional wave plates to allow analysis in arbitrary elliptical polarization bases (Fig. 2a and 2b)].

an experimental realization of this protocol, and examine various eavesdropping strategies.

We prepare the polarization-entangled state using the process of spontaneous parametric down-conversion in a nonlinear crystal [14]. In brief, two identically cut adjacent crystals (beta-barium-borate, BBO) are oriented with their optic axes in planes perpendicular to each other (Fig. 1). A 45°-polarized pump photon is then equally likely to convert in either crystal. Given the coherence and high spatial overlap (for our 0.6 mm-thick crystals) between these two processes, the photon pairs are then created in the maximally entangled state $|\phi^+\rangle$. Alice's and Bob's analysis systems each consist of a randomly driven liquid crystal (LC) (to set the applied phase shift), a half-wave plate (HWP) (with optic axis at 22.5°), and a calcite Glan-Thompson prism (PBS). Photons from the horizontal and vertical polarization outputs of each prism are detected (after narrow-band interference filters) using silicon avalanche photodiodes (EG&G SPCM-AQ's, efficiency ~60%, dark count $<400\ s^{-1}$). The correlated detector signals are synchronized and temporally discriminated through AND gates. Because of the narrow gate window (5 ns), the rate of accidental coincidences (resulting from multiple pairs or background counts) is only $10^{-5}\ s^{-1}$. From separate computers, Alice and Bob control their respective LC's with synchronously clocked arbitrary waveform generator cards [19]. A coincident event triggers a digitizer, which records the LC states, and the outputs from each of the four detector pairs [20].

Because the total rate of coincidences between Alice's and Bob's detectors was typically $5000\ s^{-1}$, the probability of having at least one pair of photons during the collection time window of 1 ms was 99%. Of course, there was then also a high probability of more than one pair being detected within the window (96%). Because the phase setting remains unchanged during a collection window, muliple pairs could conceivably give extra information to a potential eavesdropper. We avoided this problem by keeping only the first event in any given window. Assuming that Alice and Bob each have completely isolated measurement systems (i.e., there is no way for an eavesdropper to learn about the measurement parameters α and β by sending in extra photons of her own), this system is secure even though no rapid switching is employed, since only ~1 photon pair event is used for any particular α-β setting [21]. Given the 22 ms cycle period determined by the liquid crystals [22], the maximum rate of data collection in our system is 45.4 Hz. The usable rate is slightly less, because the LC voltages were occasionally in transition when the digitizer read them, yielding an ambiguous determination of the actual phase setting. Typically, we collected 40 useful pairs per second.

As seen in Table I, only 1/4 of the data actually contribute to the raw cryptographic key; half the data are used to test Bell's inequalities; and 1/4 are not used at all [23]. In four independent runs of ~10 min each, we obtained a total of 24 252 secret key bits (see Table II), corresponding to a raw bit rate of $10.1\ s^{-1}$; the corresponding bit error rate (BER) was $3.06 \pm 0.11\%$ [24]. If we attribute this BER (conservatively estimated as 3.4%) entirely to an eavesdropper, we should assume she has knowledge of up to $0.7\% + [4/\sqrt{(2)} \times 3.4\%] = 10.3\%$ (~2500 bits) of the key, where the 0.7% comes from possible double-pair events [21], and the second term assumes an intercept-resend strategy (see [8]). We must then perform sufficient privacy amplification to reduce this to an acceptable level. After running an error detection procedure on our raw key material, 18 298 error-free bits remained. Using appropriate privacy amplification techniques [6], this was further compressed to 15 444 useful secret bits (a net bit rate of $6.4\ s^{-1}$); the residual information available to any potential eavesdropper is then $2^{-(18\,298-15\,444-2500)}/\ln 2$, i.e., $\ll 1$ bit [8].

In contrast to nearly all tests of Bell's inequalities previously reported, instead of using linear polarization analyses (i.e., in the equatorial plane of the Poincaré sphere), we used elliptical polarization analysis (i.e., on the plane containing the circularly polarized poles of the sphere and the $\pm 45°$ linearly polarized states). In particular, we measured the Bell parameters [25]:

$$S = -E(\alpha_1,\beta_1) + E(\alpha_1,\beta_3) + E(\alpha_3,\beta_1) + E(\alpha_3,\beta_3), \quad (2)$$

$$S' = E(\alpha_2,\beta_2) + E(\alpha_2,\beta_4) + E(\alpha_4,\beta_2) - E(\alpha_4,\beta_4),$$

where $E(\alpha,\beta) = \frac{R_{12}(\alpha,\beta)+R_{1'2'}(\alpha,\beta)-R_{12'}(\alpha,\beta)-R_{1'2}(\alpha,\beta)}{R_{12}(\alpha,\beta)+R_{1'2'}(\alpha,\beta)+R_{12'}(\alpha,\beta)+R_{1'2}(\alpha,\beta)}$, and the R's are the various coincidence counts between

TABLE II. 100 bits of typical shared quantum key data for Alice (A) and Bob (B), generated using the Ekert protocol. Italic entries indicate errors; our average BER was 3.06%.

A: 1111100101010110100110000101001110011*0*111010100000
B: 1111100101010110100110000101001110010*0*011010101000

A: 1000100101000010*1*00111101110100100101*0*101010010111
B: 1100100101000011*1*00111101110100100101*1*101010010111

Alice's and Bob's detectors. For any local realistic theory $|S|$, $|S'| \leq 2$, while for the combinations of α and β indicated in Table I, the quantum mechanically expected values of $|S|$, $|S'|$ are $2\sqrt{2}$. In a typical 10 min run of our system, we observed $S = -2.67 \pm 0.04$ and $S' = -2.65 \pm 0.04$; for the 40 min of collected data, our combined values were $S = -2.665 \pm 0.019$, $S' = -2.644 \pm 0.019$, each a 34σ violation of Bell's inequality. It is expected (and demonstrated experimentally; see below) that the presence of an eavesdropper will reduce the observed values of $|S|$, $|S'|$. In fact, if the eavesdropper measures one photon from every pair, then $|S_{\text{eve}}| \leq \sqrt{2}$ [3]. Because we observed high values of $|S|$, $|S'|$, in our system the presence of an eavesdropper could thus be detected in $\sim$1 s of data collection (the time interval for which our $|S|$, $|S'|$ exceed $\sqrt{2}$ by 2σ). Of course, one could similarly use the BER as a check for a potential eavesdropper, who introduces a minimum BER of 25% if she measures every photon; this requires sacrificing some of the cryptographic key to accurately determine the BER.

In investigating the effects of the presence of an eavesdropper there are two main difficulties. First, there are various possible strategies; and second, we always assume that Eve has essentially perfect equipment and procedures, which of course is experimentally impossible to implement. Hence, we can at best simulate the effects she would have; we did this for two particular intercept/resend eavesdropping strategies. In the first, we make a strong filtering measurement of the polarization, in some basis χ, and send on the surviving photons to Bob. The simulated eavesdropper thus makes the projective measurement $|\chi\rangle\langle\chi|$. The effect on the measured value of S and S' and the BER depend strongly on what eavesdropping basis $|\chi\rangle$ is used [8]. Theoretical predictions and results for bases in three orthogonal planes in the Poincaré sphere are shown in Fig. 2.

The second eavesdropping strategy examined was a quantum nondemolition (QND) measurement [26]. QND measurements of *optical* photon number and polarization are presently impossible. In fact, precisely for this reason current quantum cryptography implementations *are* secure, even though they employ weak optical pulses (with *average* photon number/pulse less than 1) [27]. Nevertheless, the ideal of quantum cryptography is that it can be made secure against *any* physically possible eavesdropping strategies; hence, it is desirable to test any system against as many strategies as possible.

Although appropriate QND measurements cannot be performed at present, it is well known that their *effect* is to produce a random phase between the eigenstates of the measurement, in turn due to the entanglement of these states with the readout quantum system. We can exactly simulate this effect by inserting, in Bob's path, a birefringent element that separates the extraordinary and ordinary components of the photon wave packet by more than the coherence length ($\sim$140 μm, determined by the interference filters before the detectors); the result is a completely random phase between these polarization components, just as if a QND measurement had been made on them. Mathematically, the effect of the eavesdropper is to make a projective measurement $|\chi\rangle\langle\chi| + e^{i\langle\xi\rangle}|\chi^{\perp}\rangle\langle\chi^{\perp}|$, where $\langle\xi\rangle$ represents a random phase. Note that the theoretical predictions are identical with that for the strong polarization measurement. The experimental data are also shown in Fig. 2.

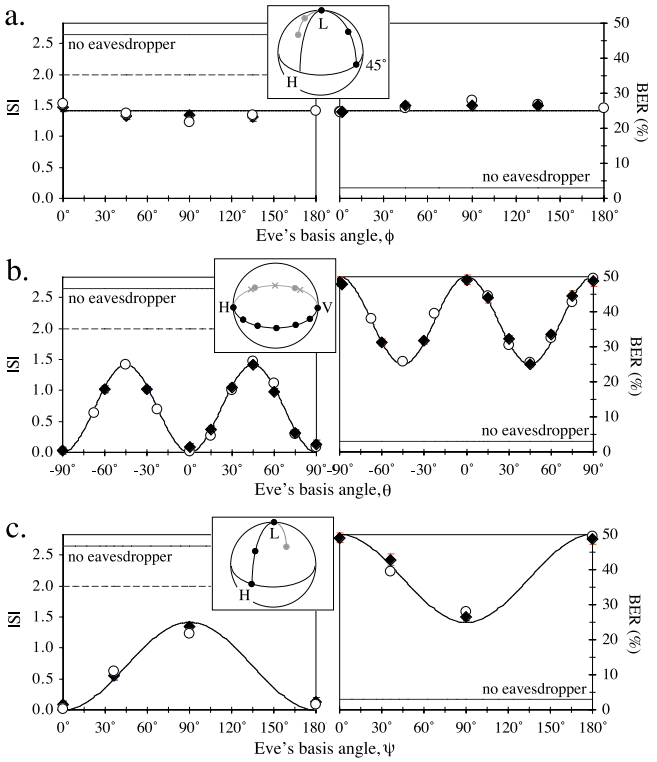

FIG. 2. Data and theory showing the effect of an eavesdropper on S and BER for various attack bases (as S' closely agrees with S, it is omitted for clarity). Diamonds represent strong measurements, made with a polarizer; circles represent QND attacks, simulated with a 3-mm-thick BBO crystal; error bars are within the points. The attack bases are (a) $|H\rangle + e^{i\phi}|V\rangle$; (b) $\cos\theta|H\rangle + \sin\theta|V\rangle$; and (c) $|45°\rangle + e^{i\psi}|-45°\rangle$; the actual measurement points in these bases are illustrated on the inset Poincaré spheres. The measured average values with no eavesdropper are indicated by unbroken grey lines, the broken lines represent the maximum classical value of $|S|$.

We see immediately that the optimal bases for eavesdropping lie in the same plane (on the Poincaré sphere) as the bases employed by Alice and Bob—for this case, the probability that the eavesdropper causes an error is "only" 25% per intercepted bit, and the $|S|$ value is $\sqrt{2}$ (Fig. 2a). On the other hand, if the eavesdropper does not know the plane of the measurement bases, and uses, e.g., random measurements in an orthogonal plane, her *average* probability of producing an error climbs to 32.5%/bit, and the average value of $|S|$ drops to $1/\sqrt{2}$. This suggests a strategy for improved security: Alice and Bob should choose bases corresponding to at least two (and ideally three) orthogonal planes, thereby "magnifying" the presence of an eavesdropper (at least one implementing

the sort of strong projective or QND-like measurement strategies investigated here) above the usual 25%/bit error probability. Quantitative theoretical investigations of such a strategy, known as the "six-state" protocol, support these claims [28].

An eavesdropper could also examine only a *fraction* of the photons, thus reducing her induced BER and increasing the S value measured by Alice and Bob, at the expense of her own knowledge of the cryptographic key. For example, if she measures (in the optimal basis) less than 58.6% of the photons, $S > 2$ and the corresponding BER $< 15\%$, but Eve's knowledge of the key will be less than Bob's (and privacy amplification techniques will still permit generation of a secret key) [29,30].

In summary, we have implemented the Ekert quantum cryptography protocol using entangled photon pairs. For this proof-of-principle experiment, Alice and Bob were situated side by side on the same optical table, obviously not the optimal configuration for useful cryptography. Nevertheless, our system demonstrates the essential features of the Ekert protocol, and moreover, we believe it is the first to *experimentally* investigate the effect of a physical intermediate eavesdropper [31]. We see no bar to extending the transmission distance to hundreds of meters [9] or even to earth-to-satellite distances [32].

We gratefully acknowledge the laboratory assistance of S. Lopez, the error correction/privacy amplification programs written by E. Twyeffort, and very helpful discussions with R. Hughes and N. Lutkenhaus.

*To whom all correspondence should be addressed.
Electronic address: Kwiat@lanl.gov

[1] P. W. Shor, SIAM Rev. **41**, 303 (1999).
[2] 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.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 773 (1993); C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, *ibid.* **41**, 1915 (1995), and references therein.
[7] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 1291 (1993); P. D. Townsend, *ibid.* **30**, 809 (1994); A. Muller *et al.,* Appl. Phys. Lett. **70**, 793 (1997); R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 549 (2000).
[8] C. H. Bennett *et al.,* J. Cryptol. **5**, 3 (1992).
[9] B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996); W. T. Buttler *et al.,* Phys. Rev. Lett. **81**, 3283 (1998).
[10] T. Durt, Phys. Rev. Lett. **83**, 2476 (1999); N. Lutkenhaus, Acta. Phys. Slovaka **49**, 549 (1999); G. Brassard, T. Mor, and B. C. Sanders, quant-ph/9906074.
[11] N. Lutkenhaus, Phys. Rev. A **59**, 3301 (1999); see also, N. Lutkenhaus, quant-ph/9910093; G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, quant-ph/9911054.
[12] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1965).
[13] P. R. Tapster, J. G. Rarity, and P. C. M Owens, Phys. Rev. Lett. **73**, 1923 (1994); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998); G. Weihs *et al.,* Phys. Rev. Lett. **81**, 5039 (1998).
[14] P. G. Kwiat *et al.,* Phys. Rev. A **60**, R773 (1999).
[15] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).
[16] A. V. Sergienko *et al.,* Phys. Rev. A **60**, R2622 (1999).
[17] During completion of our work, related results were reported by T. Jennewein *et al.,* preceding Letter, Phys. Rev. Lett. **4**, 4729 (2000), and more recently by W. Tittel *et al.,* following Letter, Phys. Rev. Lett. **4**, 4737 (2000).
[18] See, for instance, P. H. Eberhard and R. R. Ross, Found. Phys. Lett. **2**, 127 (1989).
[19] The random pulse sequences to drive the LC's were generated by LABVIEW on each of Alice's and Bob's separate computers. For our comparatively short data strings, the pseudorandom numbers were adequate.
[20] In order to average out the effect of different detector efficiencies, different detectors represented "0" and "1" depending on the phase settings, i.e., detector 1 ($2'$) represented a "0" for α_1, α_3 (β_4, β_2), but a "1" for α_2, α_4 (β_3, β_1). The resulting key contained 49% "1"s.
[21] There is a small contribution ($\sim 0.7\%$ per key bit) of events in which a double pair was emitted within the detection time (conservatively estimated as the 5 ns gate window $+35$ ns dead time). In principle an eavesdropper could learn the value of these key bits, using methods similar to those for weak pulse schemes [10].
[22] Heating the LC's to 35°, and applying "overshoot" voltages, improved the switching times to under 19 ms for all transitions; photons were collected in the following 1 ms. The cycle time could be improved to nanoseconds by using, e.g., electro-optic modulators instead of LC's.
[23] If Alice and Bob use only *three* settings and the standard Bell's inequality (as proposed by Ekert [3]), $4/9$ of the pairs go to testing Bell's inequality, and $2/9$ to the key.
[24] The BER is defined as the number of errors divided by the total size of the cryptographic key; BER $= 0.5$ implies Alice and Bob have completely uncorrelated strings.
[25] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969); A. Garuccio and V. A. Rapisarda, Nuovo Cimento Soc. Ital. Fis. **65A**, 269 (1981).
[26] M. Werner and G. Milburn, Phys. Rev. A **47**, 639 (1993).
[27] W. T. Buttler *et al.,* Phys. Rev. Lett. **83**, 2477 (1999).
[28] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1999); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[29] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997); C. A. Fuchs *et al.,* Phys. Rev. A **56**, 1163 (1997).
[30] Information lost during error correction actually reduces the BER "safety" threshold to $<11\%$ [11].
[31] The very first quantum cryptography experiment [8] simulated the effect of an intermediate eavesdropper by letting her "borrow" Alice's and Bob's apparatus, and by introducing her in the post-detection computation.
[32] R. Hughes and J. Nordholt, Phys. World **12**, 31 (1999).