New Journal of Physics
An Institute of Physics and Deutsche Physikalische Gesellschaft Journal

Entangled-photon six-state quantum cryptography

Daphna G Enzer[1,2], Phillip G Hadley[2], Richard J Hughes[2], Charles G Peterson[2] and Paul G Kwiat[2,3]

[1] Jet Propulsion Laboratory, 4800 Oak Grove Dr MS/298-100, Pasadena, CA 91109, USA
[2] Physics Division, P-23, Los Alamos National Laboratory, Los Alamos, NM 87545, USA
[3] Department of Physics, University of Illinois at Urbana-Champaign, Urbana, IL 61801-3080, USA
E-mail: kwiat@uiuc.edu

New Journal of Physics **4** (2002) 45.1–45.8 (http://www.njp.org/)
Received 1 July 2002
Published 12 July 2002

Abstract. We have implemented the 'six-state' quantum cryptography protocol using polarization-entangled photon pairs, in which the polarization of each photon of a pair is measured in one of three randomly chosen bases. For a given amount of eavesdropping, this protocol results in a larger error rate than in four- or two-state protocols, but reduces the number of key-producing events. We have experimentally investigated several incoherent eavesdropping strategies, and verified the predicted enhancement in error rate. However, we demonstrate that for low error rates, the efficiency for secret key generation is higher when using the four-state protocol.

Quantum information processing utilizes non-classical features of quantum systems to enable capabilities that would be intractable or impossible with classical techniques [1]. Quantum cryptography, or more accurately quantum key distribution (QKD), uses quantum states of photons to transfer cryptographic key material—a secret, random string of bits required to encrypt/decrypt secure communications [2]. In strong contrast with conventional methods of key distribution, the secrecy of the bit string is guaranteed by laws of physics and information theoretic methods. In a typical QKD protocol, the sender 'Alice' uses single photons [3]–[5] (or entangled photons [6, 7]) to transmit secret random bits to the receiver 'Bob'. We use polarization states, though other degrees of freedom (DOF) could also be used. Here we present the first implementation of the six-state protocol (SSP), using entangled photons, in which Alice and Bob randomly select one of three conjugate polarization bases for each photon [8]–[10]. This protocol features an increased detectability of eavesdropping at the cost of a reduction in the length of the sifted key

1367-2630/02/000045+8$30.00
© IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

(approximately two-thirds of the detected bits are in a wrong basis), so it is not obvious that the SSP has a higher or lower secret bit yield than other protocols, such as the BB84 protocol [3], which uses only two bases (four states). Our experiment incorporates several types of eavesdropping and we show that the SSP has a higher final secret bit yield [11] than BB84 only for relatively large bit error rates (BERs), in support of recent predictions [12, 13]. (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.)

In the BB84 protocol Alice encodes each random bit value using one of two non-orthogonal polarizations: for example, Horizontal (H) or $+45°$ (D) can encode a '0', while the orthogonal polarizations, Vertical (V) or $-45°$ (d), can encode a '1'. Bob randomly measures each photon's polarization in either of the two conjugate bases (H/V or D/d) and records the results. Then, by conventional public communications Alice and Bob reveal their basis choice (but not the bit value) for each detected event, and sift out the (perfectly correlated) set for which they used the same bases, and discard the uncorrelated, wrong-basis events (approximately half of the detected bits in an ideal system). If Eve intercepts every photon, measures its polarization, and sends an appropriately polarized photon on to Bob, she will induce a BER of 25–50%. The lower limit is obtained only if Eve makes her measurements in the same bases used by Alice and Bob, or in a basis that lies in the same plane on the Poincaré sphere: for example, if Alice and Bob use the (H/V) and (D/d) linear polarization bases, then eavesdropping in any linear polarization basis will yield BER = 25%. In contrast, eavesdropping in the left/right (L/R) circular polarization basis will induce a BER of 50% [7]. This observation underlies the SSP, which is structured to force Eve to make some of her measurements in a basis that induces these higher BERs, resulting in a higher overall BER (33.3%) if she intercepts every photon [8, 9].

Details of our source of polarization-entangled photon pairs are given elsewhere [14]; in brief, spontaneous parametric downconversion of a pump beam at wavelength 351 nm occurs in two adjacent non-linear crystals. The first (second) crystal can produce horizontally (vertically) polarized pairs of photons at wavelength 702 nm. Due to the coherent nature of the processes, the downconversion photons are produced in the polarization-entangled state $(|HH\rangle + |VV\rangle)/\sqrt{2}$. As shown in figure 1, Alice and Bob each receive one photon from each entangled pair, which they analyse in one of three randomly chosen bases—H/V, D/d or L/R—using a liquid crystal (LC), a Pockels cell (PC), and a calcite Glan–Thompson polarizing beam-splitting prism (PBS). LabVIEW programs generate a sequence of pseudo-random numbers and then output appropriate LC and PC control voltages in 26 ms cycles (limited by the LC response time). Toward the end of each basis-changing cycle, a 1 ms collection window is opened to look for coincidences between Alice's and Bob's detectors (silicon avalanche photodiodes). The first coincident event (dual photon detections within 5 ns) triggers a digitizer, which records both LC and PC states, as well as which one of the four detector pairs registered coincidences. The event rate is bounded by the 26 ms cycle time to only 38 s^{-1}; our measured 'raw' key generation rate was 33 s^{-1}. (Higher rates of 10^5–10^6 s^{-1} should be achievable using all electro-optic phase shifters and optimized sources.) The raw key is sifted by Alice and Bob to include only events in which they measure exactly one photon in the same basis (roughly one-third of the total events). For example, a 94 min data collection period yielded a 'sifted' key of 55 650 bits that was fairly unbiased (49% '1's), with a BER of 1.7%, comparable to the best reported error rates in past implementations of the BB84 protocol.

The main advantage of the SSP is the enhanced detectability of Eve, so one of our goals was to experimentally realize an intervening eavesdropper. A cryptographically conservative

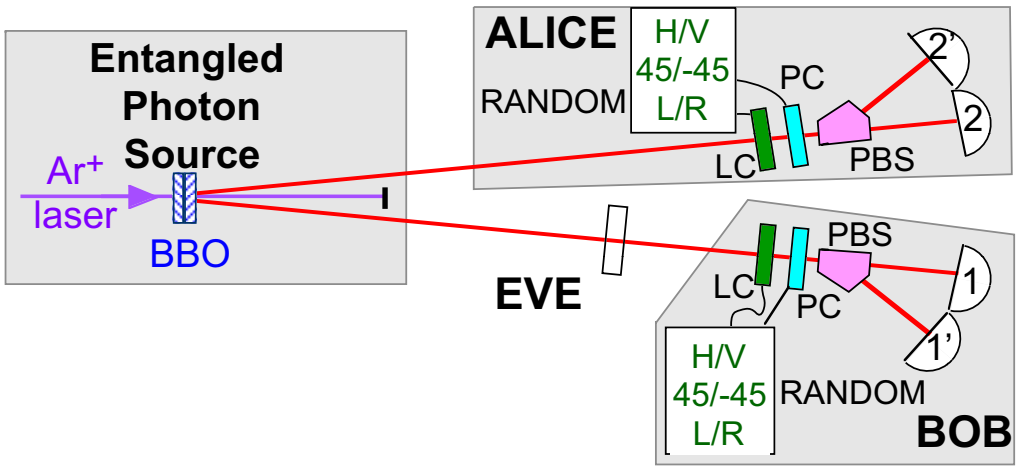

Figure 1. Entanglement-based quantum cryptography. Polarization-entangled photons produced via spontaneous parametric downconversion are directed to Alice and Bob, who detect them using high-efficiency single-photon detectors labelled $1, 1', 2,$ and $2'$ (EG&G SPCM-AQs, efficiency $\sim 60\%$, dark count $<400\ \mathrm{s}^{-1}$). Using a polarizing beam splitter (PBS) preceded by a LC and a PC, they each analyse their photons in one of three randomly chosen bases: H/V, D/d and L/R. Due to the polarization entanglement, whenever Alice and Bob choose the same basis—one-third of the time—they obtain correlated results, comprising their sifted cryptographic key material.

assumption is that Eve has perfect eavesdropping equipment, whereas we do not. With this caveat in mind, we experimentally simulated the effects of several individual bit eavesdropping strategies: strong and weak polarization measurements, and complete and partial decohering measurements. Coherent attacks on multiple photons are beyond current technology.

We simulate the first attack by placing a polarizer in the path to Bob. By using waveplates before and after the polarizer, we can make this strong projective measurement in any basis. The results shown in figure 2(a) demonstrate the effect of this 'intercept–resend' [4] attack on Alice and Bob's induced BER. Depending on the attack basis Eve uses, the BERs for the three bases used by Alice and Bob vary from ~ 0 to 50%. However, the total BER is $34.0 \pm 1.4\%$, in agreement with the predicted value 33.3%, and in contrast with 25%, the corresponding result for the BB84 protocol. In a variation, we employed glass slabs tilted at Brewster's angle to realize a partial measurement of polarization, a realization of a generalized positive-operator-valued measurement. The resulting BER curves were similar to those of figure 2(a) but peaked at only 11% and averaged to only 7%, as expected since Eve was only weakly measuring the bits.

In a delayed measurement attack, Eve entangles the photon with some ancillary quantum system (a two-qubit system is known to be optimal for the SSP [8, 9]), and waits until she overhears the public discussion between Alice and Bob to make a measurement on her ancilla. While the requisite quantum transducers and quantum memories do not exist, one can nevertheless simulate this attack by realizing that, from Alice and Bob's perspective, the net effect of such an entangling eavesdropper is to decohere the photon in the basis of her interaction. For example, if Eve couples H polarization to one state of a quantum memory and V polarization to

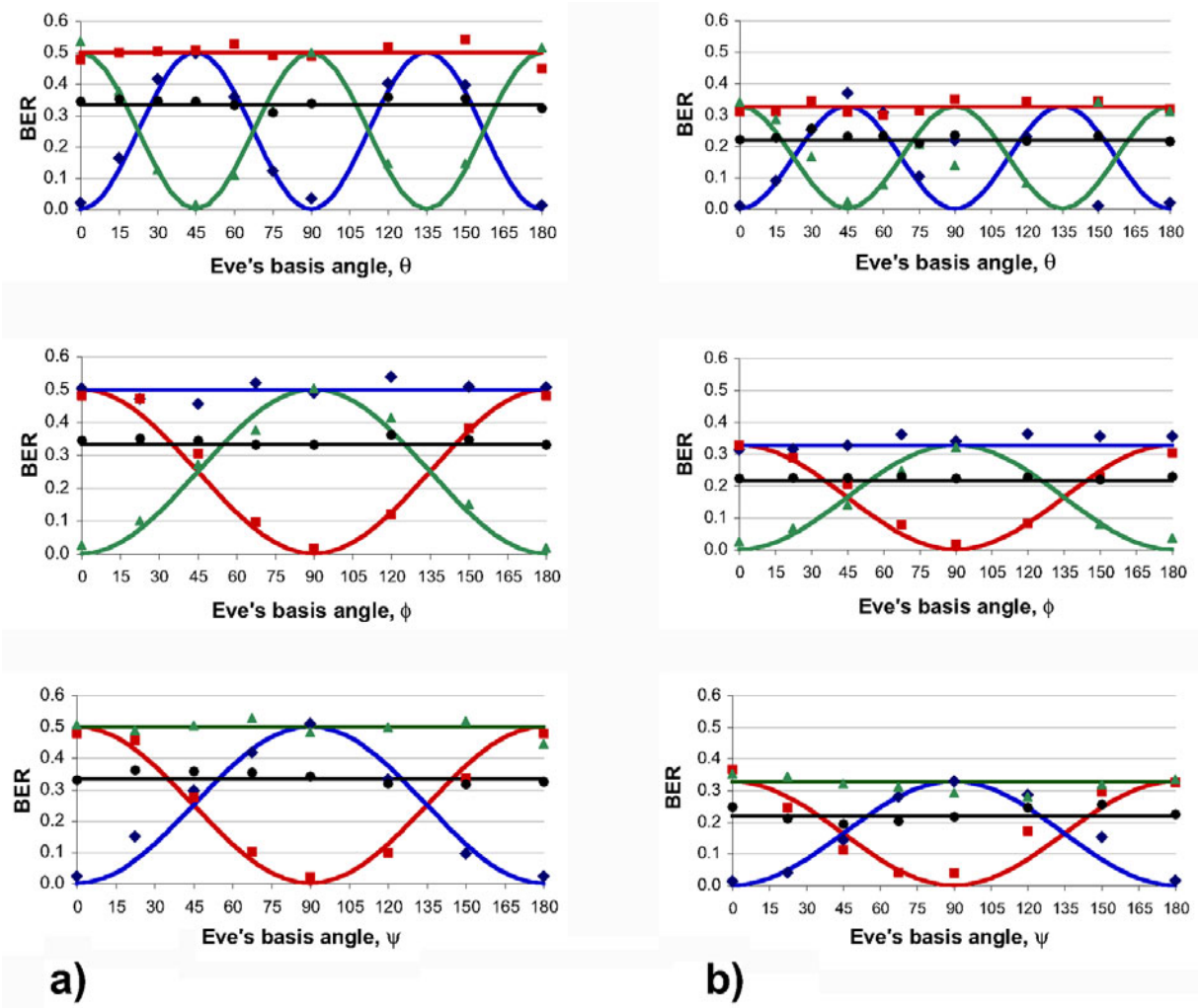

Figure 2. Alice and Bob's measured BERs for several different eavesdropping strategies. The BERs for the H/V, D/d and L/R data subsets are shown in blue, green, and red, respectively, while the total BER is shown in black. The plots' x-axes indicate the eavesdropper's attack basis. For the top, middle, and bottom plots, these bases are respectively: $\cos\theta|H\rangle + \sin\theta|V\rangle$; $|H\rangle + \mathrm{e}^{\mathrm{i}\phi}|V\rangle$; and $|D\rangle + \mathrm{e}^{\mathrm{i}\psi}|d\rangle$. In (a) we used a polarizer to implement a strong intercept–resend eavesdropping strategy; note that the total measured BER is $\sim$33%, as predicted. In (b) we used a partial decoherer (see text) to simulate an eavesdropper making a partial delayed measurement on each photon going to Bob.

another, this will effectively remove the coherence between the H and V components of Bob's photon (i.e. the photon will be left in a mixed state when we trace over the state of the memory).

Experimentally, we can realize the same effect by using a thick birefringent element. The coherence length of our detected photons is $\sim$100 μm, determined by the 5 nm (FWHM) interference filters before the detectors. A $\sim$1 cm thick piece of quartz induces a comparable relative delay between the ordinary and extraordinary polarization components, thus simulating the effect of a delayed measurement. An equivalent description is that we couple the photon's polarization

to its frequency, thus introducing a frequency-dependent phase between orthogonal polarization components. It is well known that the photons produced in spontaneous downconversion do not individually possess well-defined frequencies; therefore, after the birefringent element, the phase between the polarization components is random, just as would be the case with an entangling eavesdropper. Finally, our detectors effectively trace over the frequency—and consequently the phase—leaving the polarization of the photon in a mixed state [15, 16].

The resulting BER curves and measured BER data are essentially identical to those obtained when Eve simply measures the polarization (figure 2(a)), although Eve actually obtains more information with this more optimal attack strategy. We also simulated the more general attack of a *partially* decohering measurement by employing a thinner piece of quartz (5.7 mm)—see figure 2(b). As expected, the curves have the same form, but the total BER is reduced.

For a given attack strategy, the overall BER that Eve induces in the three bases combined is constant. However, Eve's information gain does depend on her measurement angle, even after averaging over Alice and Bob's three bases. For example, when Eve measures every photon using an intercept–resend strategy, her probability (p_E) for determining a given bit is $\max[\cos^2\theta, \sin^2\theta]$, where θ is the angle between her measurement basis and Alice and Bob's basis. Thus, the averaged p_E is between $\frac{2}{3}$ and $(\frac{1}{2}+\frac{1}{3\sqrt{2}}) \approx 0.74$ for the data shown in figure 2, but could reach as high as $(\frac{1}{2}+\frac{1}{2\sqrt{3}}) \approx 0.79$ if Eve were to measure in a direction symmetric to all three cryptographic bases: $|\chi\rangle = (|H\rangle + |D\rangle + |R\rangle)/\sqrt{3}$ [8, 9]. For each of the above eavesdropper strategies we therefore made separate measurements in this preferred symmetric basis.

We were able to directly compare these eavesdropping strategies in the SSP with BB84 by extracting a subset of the collected data for which neither Alice nor Bob used one of the bases, e.g., the LR basis. Then, for instance, the top graph in figure 2(a) only has the oscillating blue and green curves and the average BER is only 25%. In this case, Eve's information is maximized when she eavesdrops in the symmetric direction: $(|H\rangle + |D\rangle)/\sqrt{2}$.

Secret bit yields are shown in figure 3. For the cases of either no eavesdropper or an eavesdropper using the symmetric basis, we performed error correction and privacy amplification to produce final secret keys. Errors were corrected using the 'bisective search and discard' method [4, 17]. To compensate for any publicly revealed information, an appropriate number of bits were discarded during this procedure. From the BER and one of two assumed incoherent eavesdropping models (intercept–resend, and 'optimal'—coupling the photons to stored qubits), a rigorous upper bound was obtained on Eve's information. We then performed privacy amplification using a random hashing procedure [18], further reducing the (error corrected) bit string by $(1 - R)n + s$ bits, where n was the (precorrected) bit string length and R was the Renyi entropy per bit (table 1). The safety factor $s = 8$ assures that Eve's expected information is reduced below 1 bit with 99% probability [11, 19]. A few extra bits were also removed to account for possible information loss due to rare ($<0.5\%$) double-pair events.

For similar eavesdropping strategies, the effective secret key yield falls more quickly with increasing BER for BB84 than for the SSP (figure 3), because a given BER implies less information leakage to Eve in the SSP, so less has to be removed in the privacy amplification stage. However, because the SSP suffers a higher initial reduction in the sifting stage—a factor of 3 versus a factor of 2—BB84 actually has a higher yield for BERs below $\sim$8–10%. This is an example of the general phenomenon that while using more bases and possibly larger quantum systems (e.g. 3-level systems) does increase the BER induced by an eavesdropper, the useful yield of secret key material decreases, because Bob has a correspondingly smaller chance of

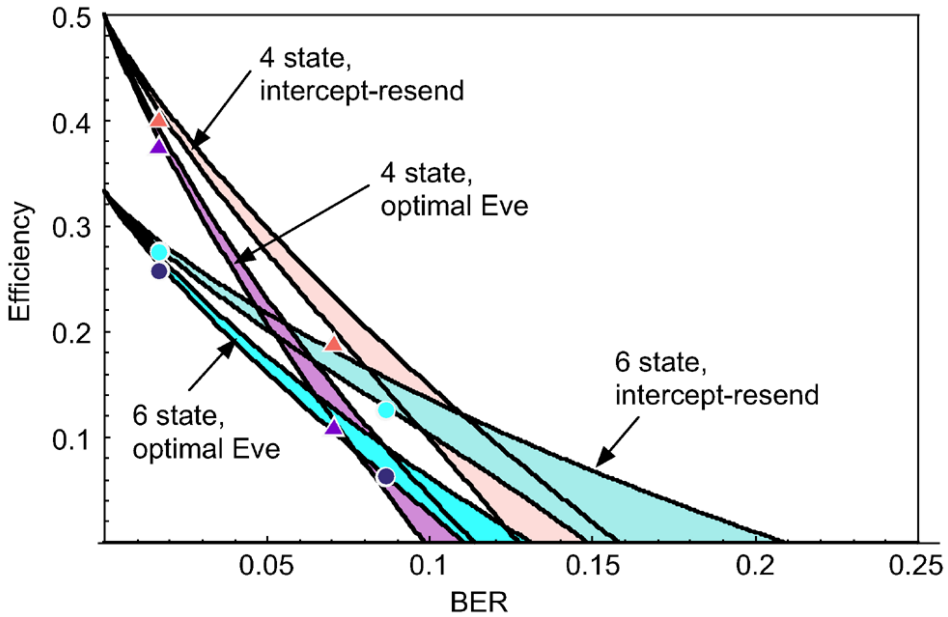

Figure 3. Secret key generation efficiencies versus BER for the four- and six-state cryptography protocols. The magenta and pink bands represent the achievable efficiencies in the four-state protocol, assuming an optimal eavesdropper and one restricted to an intercept–resend strategy, respectively. Similarly, the dark and light blue bands show the corresponding efficiencies in the SSP. The top of each band corresponds to the assumption that one could achieve the Shannon limit for information loss during error correction ($-[\epsilon \log_2 \epsilon + (1-\epsilon)\log_2(1-\epsilon)]$ bits per sifted bit, where ϵ is the BER); the bottom of each band corresponds to the best known error-correction protocol, which has more loss by a factor of $f(\epsilon) = 1.1581 + 57.200\epsilon^3$ (interpolated from table 1 in [22]). The data points show the efficiencies achieved in our experiment; efficiency is the number of secret key bits after sifting, error correction, and privacy amplification, divided by the number of unsifted valid single pair detections.

Table 1. Renyi entropy (R) quantifying Eve's ignorance per bit after using either an intercept–resend (int–r) strategy [4] or an optimal (opt) strategy ([9, 22] for BB84; [8] for SSP), where ϵ is the BER. $1 - R$ is the measure of what fraction of the string needs to be removed during privacy amplification to eliminate Eve's information, and is larger for optimal eavesdropping strategies than for intercept–resend strategies.

QKD	Eve	Renyi entropy R
BB84	int–r	$-4\epsilon \log_2[0.854^2 + 0.146^2] + (1-4\epsilon)$
BB84	opt	$-\log_2[p_E^2 + (1-p_E)^2], p_E = \frac{1}{2} + \sqrt{\epsilon(1-\epsilon)}$
SSP	int–r	$-3\epsilon \log_2[0.789^2 + 0.211^2] + (1-3\epsilon)$
SSP	opt	$-(1-\epsilon)\log_2[p_E^2 + (1-p_E)^2], p_E = \frac{1}{2} + \frac{\sqrt{\epsilon(2-3\epsilon)}}{2(1-\epsilon)}$

making his measurement in the correct basis [12]. In principle this could be remedied if he had access to a quantum memory—in the most obvious implementation, Alice would wait until Bob receives his photon, and then tell him what measurement basis to use. Thus Alice and Bob would always agree on the basis, and the SSP would always have a higher yield than BB84. It has been noted that an asymmetric weighting of Alice and Bob's bases could also increase the yield [10].

For both the SSP and BB84, the yield is substantially increased if one restricts the assumed eavesdropping strategy to intercept–resend. This is a reasonable assumption, since the optimal strategy requires presently unrealizable technologies. Lastly, although figure 3 implies there is never any yield for BERs greater than 10–15% (using the known algorithms for error correction), there are in fact two methods for increasing the tolerable error threshold. In the classical method of 'advantage distillation', Alice and Bob use public two-way communication to select a subset of their sifted key on which they agree with higher probability [20, 9]. In the completely quantum method of 'entanglement distillation', a local filtering procedure may be used on the eavesdropper-distorted entangled photons to recover a smaller number of undisturbed, maximally entangled pairs [9, 21]. In both cases, the net secret bit yield would vanish for BERs greater than 33%.

Our implementation of the SSP employed polarization-entangled photons. However, Alice could also send single photons to Bob with one of six definite polarizations. In fact, it has been argued that such a source is indistinguishable from an entangled photon source, once Alice makes her measurement [5]. Nevertheless, entangled photons offer a number of potential advantages. First, in comparison to the faint pulse sources actually employed in other experiments, the correlated photons in principle would allow secure key distribution over longer distances [2, 22], at least in fibre-based systems, which have significant attenuation and noisy detectors (at telecom wavelengths). Second, entangled photons automatically allow one to test the quality of the source [23]. Specifically, it is conceivable that some other degree of freedom (e.g. frequency) may also serve as a partial label for the polarization state. For example, if the photons with different polarizations originate in different lasers, they may have slightly different timing or frequency spectra; such a difference would in principle allow an eavesdropper to gain free information, i.e. without affecting the BER. With entangled photons, however, any DOF with which the polarization might be coupled will cause noticeable effects on the polarization correlations; any information 'leakage' to other DOFs will thus automatically manifest itself in the error rate detected by Alice and Bob. (In fact, we used precisely this phenomenon in our simulations of a delayed measurement eavesdropper.) Therefore, using only the detected error rates, one can set an upper limit on the information available to an eavesdropper, even one who is not directly measuring the polarization. However, even using entangled photons is no guarantee that there is no information leakage in the non-quantum part of the system; for example, it has recently been pointed out that some single-photon detectors actually emit photons when they have a detection event [24]. Such photons could conceivably give key information to Eve if appropriate countermeasures are not implemented.

In conclusion, we implemented the six-state quantum cryptography protocol using polarization-entangled photons, which have some advantages over non-entanglement-based schemes. We experimentally investigated several different eavesdropping attacks, demonstrating the enhanced BER sensitivity of the SSP. However, we also showed experimentally that the four-state BB84 protocol has a higher net yield of secret key bits for error rates less than $\sim 8\%$. This advantage could be removed if a quantum memory were available; the SSP's yield would then always be higher.

Acknowledgments

We wish to thank S Barraza-Lopez and N Peters for assistance, and N Gisin for helpful discussions.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Gisin N *et al* 2002 *Rev. Mod. Phys.* **74** 145
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, (Bangalore, India)* (New York: IEEE) p 175
[4] Bennett C H *et al* 1992 *J. Cryptol.* **5** 3
[5] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[6] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
Sergienko A V *et al* 1999 *Phys. Rev.* A **60** R2622
Jennewein T *et al* 2000 *Phys. Rev. Lett.* **84** 4729
Tittel W *et al* 2000 *Phys. Rev. Lett.* **84** 4737
[7] Naik D S *et al* 2000 *Phys. Rev. Lett.* **84** 4733
[8] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018
Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238
[9] Gisin N and Wolf S 1999 *Phys. Rev. Lett.* **83** 4200
[10] Lo H-K 2001 *Quant. Inform. Comput.* **1** 81
[11] Lutkenhaus N 1999 *Phys. Rev.* A **59** 3301
[12] Bruss D and Lutkenhaus N 2000 *Appl. Algebra in Eng., Commun. & Comput. AAECC* **10** 383 (*Preprint* quant-ph/9901061)
Bourennane M, Karlsson A and Bjork G 2001 *Phys. Rev.* A **64** 012306 (*Preprint* quant-ph/0106049)
Cerf N J *et al* 2002 *Phys. Rev. Lett.* **88** 127902 (*Preprint* quant-ph/0107130)
[13] Lo H-K 2001 *Preprint* quant-ph/0102138
[14] Kwiat P G *et al* 1999 *Phys. Rev.* A **60** R773
[15] Berglund A J 2000 *BA Thesis* Dartmouth College, also available on http://xxx.lanl.gov/abs/quant-ph/0010001
[16] Kwiat P G *et al* 2000 *Science* **290** 498
[17] Tancevski L *et al* 1998 *Proc. SPIE* **3228** 322
[18] Bennett C H *et al* 1995 *IEEE Trans. Inform. Theory* **41** 1915
[19] Gilbert G, Hamrick M and Thayer F J 2001 *Preprint* quant-ph/018013
[20] Maurer U M 1993 *IEEE Trans. Inform. Theory* **39** 773
[21] Kwiat P G *et al* 2001 *Nature* **409** 1014
[22] Lutkenhaus N 2000 *Phys. Rev.* A **61** 052304–1
Waks E, Zeevi A and Yamamoto Y 2002 *Phys. Rev.* A **65** 652310
[23] Mayers D and Yao A 1998 *Proc. 39th IEEE Conf. of Found. of Computer Science IEEE Comput. Soc.* p 503 (*Preprint* quant-ph/9809039)
[24] Kurtseifer C *et al* 2001 *J. Mod. Opt.* **48** 2039