Daylight Quantum Key Distribution over 1.6 km

W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson
University of California, Los Alamos National Laboratory, Los Alamos, New Mexico 87545

(Received 14 January 2000)

Quantum key distribution (QKD) has been demonstrated over a point-to-point 1.6-km atmospheric optical path in full daylight. This record transmission distance brings QKD a step closer to surface-to-satellite and other long-distance applications.

PACS numbers: 03.67.Dd, 03.65.Bz, 42.50.Ar, 42.79.Sz

Quantum cryptography was introduced in the mid-1980s [1] as a new method for generating the shared, secret random number sequences, known as cryptographic keys, that are used in crypto-systems to provide communications security (for a review, see [2]). The appeal of quantum cryptography (or more accurately, quantum key distribution, QKD) is that its security is based on laws of nature and information-theoretically secure techniques, in contrast to existing methods of key distribution that derive their security from the perceived intractability of certain problems in number theory, or from the physical security of the distribution process.

Several groups have demonstrated QKD over multikilometer distances of optical fiber [3], but there are many key distribution problems for which QKD over line-of-sight atmospheric paths would be advantageous (for example, it is impractical to send a courier to a satellite). Free-space QKD was first demonstrated in 1990 [4] over a point-to-point 32-cm tabletop optical path, and recent work has produced atmospheric transmission distances of 75 m [5] (daytime) and 1 km [6] (nighttime) over outdoor folded paths (to a mirror and back). The close collocation of the QKD transmitter and receiver in folded-path experiments is not representative of practical applications and can result in some compensation of turbulence effects. We have recently performed the first point-to-point atmospheric QKD in full daylight, achieving a 0.5-km transmission range [7], and here we report a record 1.6-km point-to-point transmission in daylight, with a novel QKD system that has no active polarization switching elements.

The success of QKD over atmospheric optical paths depends on the transmission and detection of single photons against a high background through a turbulent medium. Our results establish that the QKD photon states can be faithfully transmitted through a depth of turbulent atmosphere comparable to that encountered on a surface-to-satellite path, and that a combination of temporal, spectral [8,9], and spatial filtering [10] renders even the daylight detection problem tractable [7]. Moreover, our transmissions are of sufficient quality to support practical secret bit rates after the information-theoretic overhead required to protect against simple eavesdropping.

A QKD procedure starts with the sender, "Alice," generating a secret random binary number sequence. For each bit in the sequence, Alice prepares and transmits a single photon to the recipient, "Bob," who measures each arriving photon and attempts to identify the bit value Alice has transmitted. Alice's photon state preparations and Bob's measurements are chosen from sets of nonorthogonal possibilities. For example, using the B92 protocol [11] Alice agrees with Bob (through public discussion) that she will transmit a 45° polarized photon state $|45\rangle$, for each "0" in her sequence, and a vertical polarized photon state $|v\rangle$, for each "1" in her sequence. Bob agrees with Alice to randomly test the polarization of each arriving photon with $-45°$ polarization, $|-45\rangle$, to reveal "1s," or horizontal polarization, $|h\rangle$, to reveal "0s." In this scheme Bob will never detect a photon for which he and Alice have used a preparation/measurement pair that corresponds to different bit values, such as $|h\rangle$ and $|v\rangle$, which happens for 50% of the bits in Alice's sequence. However, for the other 50% of Alice's bits the preparation and measurement protocol uses nonorthogonal states, such as for $|45\rangle$ and $|h\rangle$, resulting in a 50% detection probability for Bob. Thus, by detecting single photons Bob identifies a random 25% portion of the bits in Alice's random bit sequence, assuming a single-photon Fock state with no bit loss in transmission or detection. This 25% efficiency factor, η_Q, is the price that Alice and Bob must pay for secrecy.

Bob and Alice reconcile their common bits by revealing the locations, but not the bit values, in the sequence where Bob detected photons; Alice retains only those detected bits from her initial sequence. In practical systems the resulting sifted key sequences [12], will contain errors; a pure key is distilled from them using classical error detection techniques. The single-photon nature of the transmissions ensures that an eavesdropper, "Eve," can neither "tap" the key transmissions with a beam splitter (BS), owing to the indivisibility of a photon [13], nor faithfully copy them, owing to the quantum "no-cloning" theorem [14]. Furthermore, the nonorthogonal nature of the quantum states ensures that if Eve makes her own measurements she will be detected through the elevated error rate she causes by the irreversible "collapse of the wave function" [15]. From the observed error rate and a model for Eve's eavesdropping strategy, Alice and Bob can calculate a rigorous upper bound on the infomation Eve might have obtained. Then, using the technique of generalized privacy

0031-9007/00/84(24)/5652(4)$15.00

amplification by public discussion [16], Alice and Bob can distill a shorter, final key on which Eve has less than one bit of information.

The QKD transmitter (Alice) in our experiment (Fig. 1) operates at a clock rate $R_0 = 1$-MHz. On each "tick" of the clock one of two temperature-controlled dim pulse "data" diode lasers emits a $\sim$1-ns optical pulse that is attenuated to the single-photon level [17] and constrained by an interference filter (IF) to 773 ± 0.5 nm to remove wavelength information. The optical paths from each data laser are matched to $<$2 mm to remove timing information. Polarizers set one data laser's output to be 45° polarized and the other to be vertically polarized as required for the B92 protocol. The choice of which data laser fires is determined by a random bit value that is obtained by discriminating electrical noise. The random bit value is indexed by the clock tick and recorded in Alice's computer control system's memory. After a short 5-ns delay [18] a 5-ns vertically polarized optical "bright pulse" is produced from a "timing-pulse" diode laser whose wavelength is temperature controlled to $\sim$768 nm. All three optical pulse paths are combined with BSs into a single-mode (SM) optical fiber to remove spatial mode information, and transmitted toward Bob's receiver through a 27× beam expander that extends the system Rayleigh range. A single-photon detector (SPD) [19] located behind a matched IF in one of the BS output ports is used to monitor the average photon number $\bar{n}$ of the dim pulses as follows: (1) a calibration photon-number measurement is made from the rate at which a calibrated single-photon counting module (SPCM) [20] fires at the transmitter's SM transmission-fiber output with a given input, (2) next the transmitter's SPD count rate is calibrated to the SPCM firing rate with the same input to determine the SPD efficiency, which is then (3) used with the experimental SPD count rates to measure the transmitted $\bar{n}$ in key generation mode.

At the QKD receiver (Bob) light pulses are collected by a 8.9-cm diameter Cassegrain telescope and directed into a polarization analysis and detection system (Fig. 2). A bright pulse triggers a "warm" avalanche photodiode (APD), which sets up a narrow $\sim$5 ns coincidence gate in which to test a subsequent dim pulse's polarization [18]. A BS randomly directs dim pulses along one of two paths. Polarization elements along the upper path are set to transmit $-45°$ polarization in accordance with Bob's B92 "1" value, while along the lower path a measurement for $|h\rangle$ to reveal "0"s is made using a polarizing beam splitter (PBS). (The PBS transmits $|h\rangle$ but reflects $|v\rangle$.) Each analysis path contains a matched IF and couples to a SPD via multimode (MM) fiber that provides limited spatial filtering, giving the receiver a restricted 200 μ-radian field of view. For events on which one of the two SPDs triggers during the coincidence gate, Bob can assign a bit value to Alice's transmitted bit; upper-path SPD firings identify "1"s, and lower-path SPD firings identify "0"s. He records these detected bits in the memory of his computer control system, indexed by the "bright pulse" clock tick. Bit generation is completed when Bob communicates the locations, but not values, of his photon detections in Alice's random bit sequence over a public channel: wireless ethernet in our experiment.

The QKD system was operated over a 1.6-km outdoor range with excellent atmospheric conditions on Friday 13 August 1999 beginning at 09:30 local standard time (LST) under cloudless New Mexico skies. By 11:30 LST turbulence induced beam-spreading hindered our ability to efficiently acquire data at low bit-error rates (BER), ϵ (where BER, ϵ, is defined as the ratio of the number of bits received in error to the total number of bits received). The system efficiency, η_{sys}, which accounts for losses between the transmitter and MM fibers at the receiver, and the receiver's SPDs efficiencies had an average value of $\langle \eta_{\mathrm{sys}} \rangle \sim 0.13$ with a standard deviation of $\sigma = 0.04$. Fluctuations in η_{sys} were caused by turbulence induced beam spreading and beam wander; the typical beam

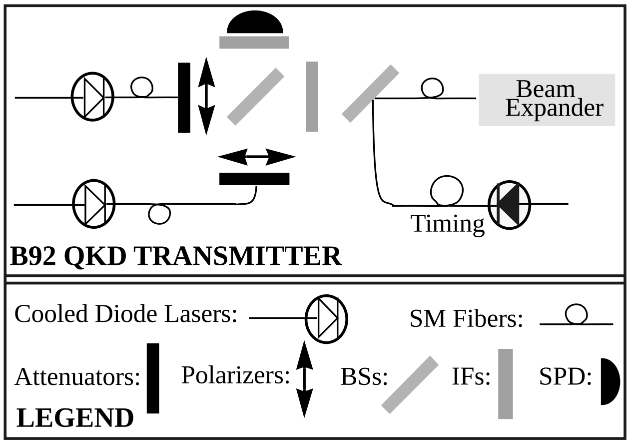

FIG. 1. Free-Space QKD Transmitter (Alice): The legend describes the basic components; cooled data lasers (on left) are pulsed 5 ns prior to the timing laser. See text for details.

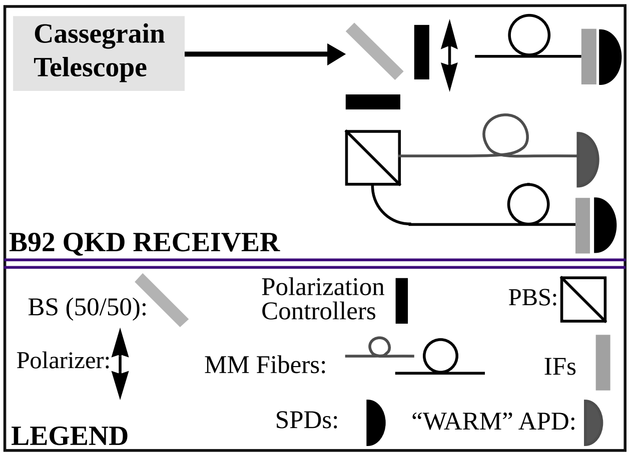

FIG. 2. Free-Space QKD Receiver (Bob): The legend describes the basic components; SPD MM-fibers are longer than the "warm" APD MM-fiber to delay the dim pulse 10 ns relative to the bright timing-pulse. See text for details.

wander was observed to be on the order of 3 to 5 μrad. (Our present system has no beam-steering or adaptive-optics technology to compensate for turbulence-induced effects.) The $\eta_Q = 0.25$ quantum efficiency of the B92 protocol lowers the overall efficiency to $\eta = \eta_Q \eta_{\text{sys}} \sim 0.0325$ and leads to a detection probability for Bob of $P_B = 1 - \exp(-\eta \bar{n})$. This gave a bit rate of $R \sim 5.4$, 12.2, and 17 kHz at $\bar{n} \sim 0.2$, 0.35, and 0.5 photons per dim pulse, respectively, when the lasers were pulsed at $R_0 = 1$ MHz. Bits were transmitted in 25, 50, and 100 kbit blocks. A total of 1.55 Mbit were sent in 40 data exchanges between Alice and Bob and 17 420 bits of sifted key were received. Table I includes a typical 250-bit sample from one of several 1.6-km daylight transmissions on 13 August 1999. The sifted key shown contains eight bit errors (in bold) corresponding to $\epsilon = 3.2\%$ for these 250 bits and has a 60:40 bias toward ones (the average bias for all experiments on 13 August 1999 was 50.3:49.7 toward ones). The average BER on all key material acquired during the daylight transmissions was $\langle \epsilon \rangle = 5.3\%$. These BERs would be regarded as unacceptably high in any conventional telecommunications application but are tolerated in QKD because of the secrecy of the bits.

The dominant BER component is from the ambient solar background, with a measured noise probability for both detectors of about 6.7×10^{-4} per coincidence gate, contributing about 5.9% to the $\langle \epsilon \rangle = 7.8\%$ at $\bar{n} = 0.2$ data, about 2.4% to the $\langle \epsilon \rangle = 4.1\%$ at $\bar{n} = 0.35$, and about 1.9% to the $\langle \epsilon \rangle = 4.1\%$ at $\bar{n} = 0.5$. (The ambient background is somewhat less than that expected from the daylight radiance [6], which we attribute to Bob viewing the dark interior of the tent housing Alice's transmitter.) Imperfections and misalignments of the polarizing elements were the next largest contribution (about 1.9%) to the total BERs on 13 August 1999. Experience from previous experiments [6,7,10] suggests that this component of BER can be reduced to about 0.5%. Detector dark noise ($\sim$1 400 dark counts per second) makes an even smaller contribution of <0.1% to the BER. The dual-fire rate—the probability that both SPDs fire during a coincidence window—was 0.0003, 0.0007, and 0.001 at $\bar{n} \sim 0.2$, 0.35, and 0.5, respectively.

TABLE I. A 250-bit sample of Alice's (a) and Bob's (b) raw key material generated at Los Alamos, New Mexico at 10:00 LST (GMT − 7) on Friday 13 August 1999. Alice was located at 1978-m elevation, 35° 46.859′ N, and 106° 14.932′ W; Bob was located at 1966-m elevation, 35° 46.376′ N, and 106° 14.052′ W. The beam height at Alice's transmitter and Bob's receiver was 1.5-m; the maximum beam height of 107-m above the terrain occurred 1 km from Alice, and the average beam height above the terrain was ~38-m.

a	00011011110111010111010000101011111101111101110000
b	**1**0011011110**0**1101011**0**01**1**000101011111101111101110000
a	01111110111100011011000010111101110010000101001010
b	011111101**0**11000110110000**0**0111101110010000101001010
a	00011110111110000100011111001111011011011101101111
b	0001111011**0**110000100011111001111011011011101101111
a	10010010100100100100111100000001101001111100101111
b	10010010100100100100111100000001101001111100101**0**11
a	11111111111111111000011111011101101110101100011101
b	11111111111111111000011111011101101110101100011101

Alice and Bob can correct errors by transmitting error correction information over the public channel, amounting to

$$f(\epsilon) = -\epsilon \log_2 \epsilon - (1 - \epsilon) \log_2 (1 - \epsilon) \tag{1}$$

bits per bit of sifted key in the Shannon limit. For example, for $\epsilon = 4.1\%$, $f(0.041) = 0.246$. Practical error-correcting codes do not achieve the Shannon limit, although the interactive scheme known as CASCADE [21], comes within about $1.16 f(\epsilon)$ for error rates up to 5% [12]. Our experiments use a combination of block-parity checks and Hamming codes [22] achieving an efficiency equivalent to the CASCADE scheme but with greater computational efficiency. The error correction information is transmitted over the public channel and thus could provide information about the key material to Eve, reducing Alice and Bob's secret bit yield. (Alice and Bob could encrypt the error correction information to deny Eve access to it, but at the cost of an equal number of shared secret key bits [23].)

Alice and Bob now use "privacy amplification" [16] to reduce any partial knowledge gained by an eavesdropper to less than 1 bit of information. (For discussions of eavesdropping strategies, see Refs. [12,24,25].) We have not implemented privacy amplification at this time, but to estimate the secret-key rate for our experiment and its dependencies on relevant parameters, we assume Eve is restricted to performing the combination of the intercept-resend and beam splitting attacks considered in [4]. In this case Alice and Bob could use the parities of random subsequences of their error-corrected keys as their final secret key bits, resulting in a compression to

$$F(\epsilon) = (1 - \bar{n}) - 2\sqrt{2}\,\epsilon \tag{2}$$

bits per bit of error-corrected key, where we have (conservatively) assumed that Eve identifies every multiphoton pulse. The first term in Eq. (2) accounts for the multiphoton fraction of Alice's dim pulses, which are susceptible to beam splitting, while the second accounts for Eve performing intercept resend on a fraction of the pulses. The final secret bit yield is therefore a fraction $F(\epsilon) - f(\epsilon)$ the length of the original sifted key. For $\bar{n} \lesssim 0.05$, under the conditions of our 13 August 1999 experiment with $\eta_{\text{sys}} = 0.13$, there is no net secret bit yield because of the large value $f(\epsilon)$. With increasing $\bar{n}$ the BER decreases so rapidly that the increased privacy amplification cost to protect against beam splitting is more than offset by the reduced error-correction cost, and so the secret bit yield initially increases. However, for larger $\bar{n}$ values, the privacy amplification factor $F(\epsilon)$ required to compensate for beam splitting of multiphoton pulses becomes small, and the secret bit yield decreases, vanishing for $\bar{n} \gtrsim 0.7$. For $\eta_{\text{sys}} = 0.13$, we find that the optimum $\bar{n}$ for our 13 August 1999 experiment is $\sim$0.4, giving a secret bit yield of 38.5% of the sifted key length, and $\sim$0.4% of the length of the transmitted sequence. (With CASCADE or our block-parity/Hamming code combination the optimal $\bar{n}$ would also be $\sim$0.4 and the secret bit yield would be 24.7% of the sifted key or 0.32% the length of the transmitted sequence, giving a secret bit rate of $\sim$3 kHz.) For smaller η_{sys} values under 13 August 1999 conditions the optimal $\bar{n}$ values are as above but the secret bit yield is smaller; for $\eta_{\text{sys}} < 0.04$ there is no secret bit yield. (To protect against the attacks proposed in [12], should they become feasible, we would need to reduce our background further with a shorter coincidence gate window and narrower spectral filters to have a nonzero secret-bit yield at the $\bar{n}$ values required.)

This Letter reports QKD between a transmitter and receiver separated by a 1.6-km daylight atmospheric optical path. Secret bit rates of several kilohertz protected against simple beam splitting and intercept-resend attacks have been shown to be feasible. Such rates would enable the rekeying of cryptographic systems [7]. Our system has no active polarization elements, resulting in greater simplicity and security over previous experiments, and could be easily adapted to the BB84 four-state QKD protocol [1] or to use single-photon light sources [26] once they are available, providing protection against more sophisticated future attacks [12,24,25]. Our transmission distance, which was limited only by the length of the available range, is the longest to date, and is representative of practical situations showing that QKD could be used in conjunction with optical communication systems. The turbulence encountered along our 1.6-km optical path is comparable to the effective turbulent atmospheric thickness in a surface-to-satellite application so that our results provide evidence for the feasibility of surface-to-satellite QKD [7]. Significant amounts of key material (about 15 kbits) with low BERs ($\langle\epsilon\rangle \lesssim 3.0\%$) at low $\bar{n}$ ($\bar{n} \lesssim 0.2$) were also taken at night and during light rain over this 1.6-km distance. Finally, we note that the variability of system efficiency and background is a feature of atmospheric QKD that is quite different from optical fiber systems.

We thank P. G. Kwiat for QKD discussions, D. Derkacs for technical support, and G. H. Nickel, D. Simpson, and E. Twyeffort for discussions regarding bit-error detection protocols and privacy amplification.

---

[1] 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.

[2] R. J. Hughes *et al.*, Contemp. Phys. **36**, 149 (1995).

[3] J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994); C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995); R. J. Hughes *et al.*, Lect. Notes Comput. Sci. **1109**, 329 (1996); A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996); R. J. Hughes *et al.*, Proc. SPIE Int. Soc. Opt. Eng. **3076**, 2 (1997); R. J. Hughes *et al.*, J. Mod. Opt. **47**, 533 (2000).

[4] C. H. Bennett *et al.*, Lect. Notes Comput. Sci. **473**, 253 (1990); C. H. Bennett *et al.*, J. Crypt. **5**, 3 (1992).

[5] B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).

[6] W. T. Buttler *et al.*, Phys. Rev. Lett. **81**, 3283 (1998).

[7] R. J. Hughes *et al.*, J. Mod. Opt. **47**, 549 (2000); R. J. Hughes and J. E. Nordholt, Phys. World **12**, 31 (1999).

[8] J. G. Walker *et al.*, Quantum Opt. **1**, 75 (1989).

[9] S. F. Seward *et al.*, Quantum Opt. **3**, 201 (1991).

[10] W. T. Buttler *et al.*, Phys. Rev. A **57**, 2379 (1998).

[11] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[12] N. Lutkenhaus, quant-ph/9910093 (1999); G. Brassard *et al.*, quant-ph/9911054.

[13] J. F. Clauser, Phys. Rev. D **9**, 853 (1974).

[14] W. K. Wooters and W. H. Zurek, Nature (London) **299**, 802 (1982); P. W. Milonni and M. L. Hardies, Phys. Lett. **92A**, 321 (1982).

[15] A. K. Ekert *et al.*, Phys. Rev. A **50**, 1047 (1994).

[16] C. H. Bennett *et al.*, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[17] The attenuated pulse only approximates a “single-photon” Fock state. Dim pulses of $\bar{n} \sim 0.3$ have a 2-photon probability of $\sim$0.04, implying $\sim$18% of detectable pulses contain more than one photon.

[18] In this atmospheric QKD system, Alice transmits dim pulses *before* the timing pulses to reduce noise caused by system reflections, but Bob detects dim pulses *after* the bright pulses by using longer MM fibers on the key-bit detector paths to delay the dim pulses.

[19] Our SPDs are based on EG&G Canada Ltd., Optoelectronics Division, product #C30902S, and have a single photon detection efficiency of $\eta_{\text{spd}} \sim 0.69$ at 773 nm, and a dark count rate $\sim 1400\ \text{s}^{-1}$.

[20] The MM fiber-coupled SPCM is a EG&G Canada Ltd., Optoelectronics Division, product and has a single photon detection efficiency of $\eta_{\text{spcm}} \sim 0.44$ at 773 nm, and a dark count rate $<100\ \text{s}^{-1}$.

[21] G. Brassard and L. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994).

[22] R. W. Hamming, *Coding and Information Theory* (Prentice Hall, New Jersey, 1980).

[23] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).

[24] T. Durt, Phys. Rev. Lett. **83**, 2476 (1999).

[25] W. T. Buttler *et al.*, Phys. Rev. Lett. **83**, 2477 (1999).

[26] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986); J. Kim *et al.*, Nature (London) **397**, 500 (1999); C. Brunel *et al.*, Phys. Rev. Lett. **83**, 2722 (1999).