LA-UR- 98-3962

Approved for public release; distribution is unlimited.

Title: FREE-SPACE QUANTUM CRYPTOGRAPHY

CONF-980897--

Author(s): R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson

Submitted to: Proceedings of the "Quantum Communications and Measurement" conference, Northwestern University, Evanston, IL, August 23-27, 1998

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

Free-space quantum cryptography

R. J. Hughes, W. T. Buttler, P. G. Kwiat, 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, USA

Abstract

An experimental free-space quantum key distribution (QKD) system has been tested over an outdoor optical path of $\sim$ 1 km under nighttime conditions at Los Alamos National Laboratory. This system employs the Bennett 92 protocol; here we give a brief overview of this protocol, and describe our experimental implementation of it. An analysis of the system efficiency is presented, as well as a description of our error detection protocol, which employs a two-dimensional parity check scheme. Finally, the susceptibility of this system to eavesdropping by various techniques is determined. Possible applications include the rekeying of satellites in low earth orbit.

INTRODUCTION

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. The appeal of quantum cryptography is that its security is based on laws of Nature, in contrast to existing methods of key distribution that derive their security from the perceived intractability of certain problems in number theory,[2] or from the physical security of the key distribution process.

Since the introduction of quantum cryptography, several groups have demonstrated quantum communications[3,4] and key distribution[5–10] over multi-kilometer distances of optical fiber. Free-space QKD (over an optical path of 32 cm) was first introduced in 1991,[11] and recent advances have led to demonstrations of QKD over free-space indoor optical paths of 205 m,[12] and outdoor optical paths of 75 m.[13] These demonstrations increase the utility of QKD by extending it to line-of-site laser communications systems. Indeed there are certain key distribution problems in this category for which free-space QKD would have definite practical advantages (for example, it is impractical to send a courier to a satellite). Here we report our results of free-space QKD over outdoor optical paths of up to 950 m under nighttime conditions.[14]

Table 1. Observation Probabilities

Alice's Bit Value Bob Tests With	"0" "1"	"0" "0"	"1" "1"	"1" "0"
Observation Probability	p= 0	p= $\frac{1}{2}$	p= $\frac{1}{2}$	p= 0

The Bennett 92 Protocol

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 non-orthogonal possibilities. For example, using the B92 protocol[18] Alice agrees with Bob (through public discussion) that she will transmit a horizontal-polarized photon, $|h\rangle$, for each "0" in her sequence, and a right-circular-polarized photon, $|r\rangle$, for each "1" in her sequence. Bob agrees with Alice to randomly test the polarization of each arriving photon with vertical polarization, $|v\rangle$, to reveal "1s," or left-circular polarization, $|\ell\rangle$, 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 protocols use non-orthogonal states, such as $|h\rangle$ and $|\ell\rangle$, resulting in a 50% detection probability for Bob, as shown in Table 1. 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 reception. This 25% efficiency factor, η_Q, is the price that Alice and Bob must pay for secrecy.

Bob and Alice reconcile their common bits through a public discussion 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. The resulting detected bit sequences comprise the raw key material from which a pure key is distilled 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,[19] nor copy them, owing to the quantum "no-cloning" theorem.[20] Furthermore, the non-orthogonal 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 wavefunction.[21]"

Quantum-Key Transmitter: Alice

The faithful transmission of polarized single photons through a turbulent medium (the atmosphere), receiving them with non-negligible probability and detecting them against a high ambient background, appear to be serious obstacles to free-space QKD. However, these obstacles can be overcome by exploiting sub-nanosecond timing techniques, narrow wavelength filters,[15,16] spatial filtering,[12,14] and adaptive optics.[17]

The QKD transmitter for our experiments (Fig. 1) consisted of a temperature-controlled single-mode (SM) fiber-pigtailed diode laser, a fiber to free-space launch system, a 2.5-nm bandwidth interference filter (IF), a variable optical attenuator, a polarizing beam splitter (PBS), a low-voltage Pockels cell, and a 27× beam expander. The diode laser wavelength is temperature adjusted to 772 nm, and the laser is con-

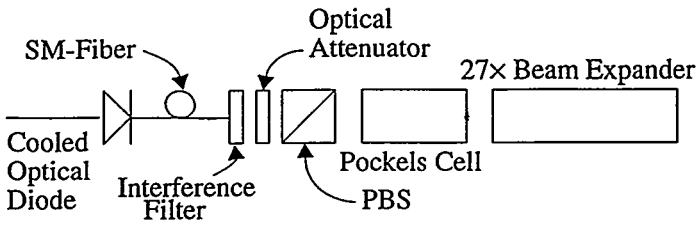

Figure 1. QKD Transmitter.

figured to emit a short, coherent pulse of approximately 1-ns length, containing $\sim 10^5$ photons.

A computer control system (Alice) starts the QKD protocol by pulsing the diode laser at a rate previously agreed upon between herself and the receiving computer control system (Bob). Each laser pulse is launched into free-space through the IF, and the $\sim$ 1 ns optical pulse is then attenuated to an average of less than one photon per pulse, based on the assumption of a statistical Poisson distribution.[22] (The attenuated pulse only approximates a "single-photon" state; we tested the system with averages down to less than 0.1 photon per pulse. This corresponds to a 2-photon probability of $< 0.5\%$ and implies that less than 6 of every 100 detectable pulses will contain 2 or more photons, i.e., for a Poisson distribution with an average photon number of $\bar{n} = 0.1$, for every 1000 pulses there will be $\sim$ 905 empty pulses, $\sim$ 90 pulses of 1 photon, $\sim$ 5 pulses of 2 photons, and $\sim$ 1 pulse of 3 or more photons.) The photons that are transmitted by the optical attenuator are then polarized by the PBS, which transmits an average of less than one $|h\rangle$ photon to the Pockels cell. The Pockels cell is randomly switched to either pass the "single-photon" unchanged as $|h\rangle$ (zero-wave retardation) or change it to $|r\rangle$ (quarter-wave retardation). The random switch setting is determined by discriminating the voltage generated by a white noise source.

Quantum-Key Receiver: Bob

The free-space QKD receiver (Fig. 2) comprised a 8.9 cm Cassegrain telescope followed by the receiver optics and detectors. The receiver optics consisted of a 50/50 BS that randomly directs collected photons onto either of two distinct optical paths. The lower optical path contained a polarization controller (a quarter-wave retarder and a half-wave retarder), adjusted as an effective quarter-wave retarder, followed by a PBS to test collected photons for $|h\rangle$ (at first glance this may be confusing, but the effective quarter wave retarder converts $|h\rangle$ to $|r\rangle$ leading to a 50% probability an $|h\rangle$ photon will be detected); the upper optical path contained a half-wave retarder followed by a PBS to test for $|r\rangle$. The output port along each optical path was coupled by multi-mode (MM) fiber to a single-photon counting module (SPCM: EG&G part number: SPCM-AQ 142-FL). [Although the receiver did not include IFs, the spatial filtering provided by the MM fibers effectively reduced noise caused by the ambient background during nighttime operations to negligible levels (the background was $\sim$ 1.1 kHz).]

Bit values are determined in the following fashion: a single $|r\rangle$ photon traveling along the lower path encounters the polarization controller, and is converted to $|v\rangle$ and reflected away from the SPCM by the PBS, but a single $|h\rangle$ photon traveling the same path is converted to $|r\rangle$ and transmitted toward or reflected away from the SPCM in this path with equal probability; in contrast, a single $|h\rangle$ photon traveling the upper path is converted to $|v\rangle$ and reflected away from the SPCM in this path, but a single

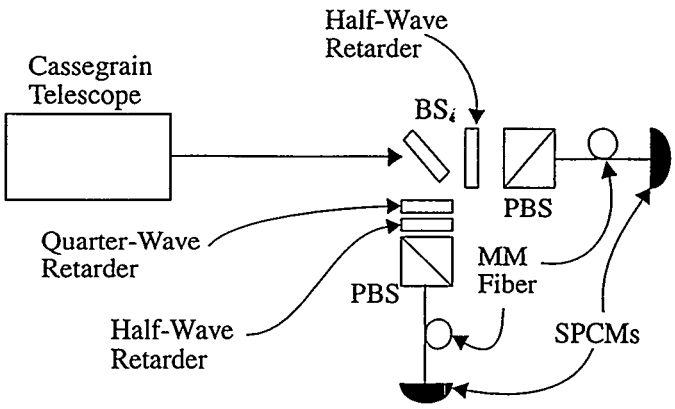

Figure 2. QKD receiver.

$|r\rangle$ photon traveling this path is converted to $|\ell\rangle$ and transmitted toward or reflected away from the SPCM with equal probability.

In this detection scheme, there are a total of four possible optical paths through the receiver, but only two of the paths, those which terminate upon the detectors seen in Fig. 2, contain definite polarization information (definite in the sense that Bob can know what polarization Alice has transmitted if one of these detectors fire). However, while the remaining two paths contain indeterminate polarization information (indeterminate in the sense that Bob cannot know with certainty whether Alice has transmitted $|h\rangle$, or $|r\rangle$ if a detector placed in either of these paths fires), this information remains important for the secure implementation of B92.

Outdoor Free-Space Experiments

The transmitter and receiver optics were operated over 240-, 500-, and 950-m outdoor optical paths, with the transmitter and receiver collocated in order to simplify data acquisition. The various total optical path lengths were determined by positioning a 25.4 cm diameter mirror at the transmission distance half way point that reflected the transmitted beam back to the receiver. All measurements were made at night.

System Efficiency

The optical coupling efficiency between the transmitter and receiver for the 950-m path was $\eta \sim 14\%$, which accounts for losses between the transmitter and the MM fibers at the receiver. Bob's detection probability,

$$P_B = e^{-\bar{n}} \sum_{n=1}^{\infty} \frac{\bar{n}^n}{n!} [1 - y^n] = 1 - e^{-\bar{n}\eta_B}, \tag{1}$$

is the convolution of the Poisson probability distribution of photons in Alice's transmitted weak pulse with average photon number $\bar{n}$, and the probability that Bob detects at least 1 photon. Here, $y = (1 - \eta_B)$, where $\eta_B = \eta \cdot \eta_D \cdot \eta_Q$, and $\eta_D = 65\%$ is Bob's detector efficiency. When the transmitter was pulsed at a rate of 20 kHz with an average of 0.1 photon per pulse for the 950-m path, Eq. 1 gives $\bar{n} \cdot \eta_B = 0.1 \cdot (0.14 \cdot 0.25 \cdot 0.65) \sim 2.3 \times 10^{-3}$, and hence a bit rate in agreement with the experimental result of ~ 50 Hz.

The bit error rate (BER, defined as the ratio of the bits received in error to the total number of bits received) for the 950-m path was $\sim 1.5\%$ when the system was

Table 2. A 200-Bit Sample of Alice's (A) and Bob's (B) Raw Key Material Generated by QKD over 1 km.

A	0000010101	1101101001	0000000000	0110010101
B	0000010101	1101101001	0000000000	0110010101
A	0011100010	0111011101	1110111000	0100100011
B	0011100010	0111011101	1110111000	0100100011
A	1110000000	0101101111	1001001010	0010000011
B	1110000000	0101101111	1001001010	0010000011
A	0000010111	0000111111	1111000000	1010101101
B	0000010111	0000111111	1101000000	1010101101
A	1111100111	1110111101	0100110100	1011101111
B	1111100011	1110111101	0100110100	1011101111

operating down to < 0.1 photon per pulse level. (A BER of $\sim 0.7\%$ was observed over the 240-m optical path and a BER of $\sim 1.5\%$ was also observed over the 500-m optical path.) A sample of raw key material from the 950-m experiment, with errors, is shown in Table 2.

Bit errors caused by the ambient background were minimized to less than ~ 1 every 9 s by narrow gated coincidence timing windows (~ 5 ns) and spatial filtering. Further, because detector dark noise (~ 80 Hz) contributed only about 1 dark count every 125 s, we believe that the observed BER was mostly caused by misalignment and imperfections in the optical elements (wave-plates and Pockels cell).

Error Detection

Our experiments implement a two-dimensional (2D) parity check scheme that allows the generation of error-free key material. Error detection is accomplished by Bob and Alice organizing their reconciled bits into 2D square matrices in the order that they were detected. Once organized, the parities of the rows and columns are determined and openly exchanged between Alice and Bob, and any column or row in which Bob and Alice possess different parities is discarded. To ensure privacy, Alice and Bob also discard the bits oriented along the diagonals of their matrices. This guarantees the elimination of two bits for each row and column of the matrix, even when no errors are detected, eliminating knowledge revealed during the parity exchange.

Eavesdropping by Eve

The original form of the B92 protocol has a weakness to an opaque attack by Eve. For example, Eve could measure Alice's photons in Bob's basis and only send a dim photon pulse when she identifies a bit. However, if Eve retransmits each observed bit as a single-photon she will noticeably lower Bob's bit-rate. To compensate for the additional attenuation to Bob's bit-rate Eve could send on a dim photon pulse of an intensity appropriate to raise Bob's bit-rate to a level similar to her own bit-rate with Alice. [In fact, if Eve sends a bright classical pulse (a pulse of a large average photon number) she guarantees that Bob's bit-rate is close to her own bit-rate with Alice.] However, this type of attack would be revealed by our two SPCM system through an increase in "dual-fire" errors, which occur when both SPCMs fire simultaneously. In a

perfect system dual-fire errors would not exist, regardless of the average photon number per pulse, but in a real experimental system, where bit-errors occur, dual-fire errors will occur. (We have used the dual-fire information to estimate the average number of photons per pulse reaching the SPCMs.) Our system could also be modified to operate under the BB84 protocol[1] which also protects against an opaque attack.

Eve could also passively, or translucently, attack the the system using a BS and a receiver identical to Bob's (perhaps of even higher efficiency) to identify some of the bits for which Alice's weak pulses contain more than 1 photon, i.e., Eve receives pulses reflected her way by the BS which has reflection probability R, whereas Bob receives the transmitted pulses, and the BS has transmission probability $T = 1 - R$. Introducing a coupling and detection efficiency factor η_E, for Eve, analogous to Bob's η_B, we find that Eve's photon detection probability is $P_E = 1 - e^{-\bar{n}\,\eta_E\,R}$, whereas Bob's detection probability becomes $P_B = 1 - e^{-\bar{n}\,\eta_B\,T}$. (Note: we do not explicitly consider any eavesdropping strategy, with or without guessing, in which Eve might use more than 2 detectors.)

The important quantity in a BS attack is the ratio of the number of bits Eve shares with Bob to the number of bits Bob and Alice share. We find that the probability that Eve and Bob will both observe a photon on the same pulse from Alice is[23,24]

$$P_{B\wedge E} = [1 - e^{-\bar{n}\,\eta_E\,R}]\,[1 - e^{-\bar{n}\,\eta_B\,T}]\,. \tag{2}$$

To take an extreme case, if Eve's BS has $R = 0.9999$, her efficiency is perfect (i.e., $\eta_E = 0.25$), and Alice transmits pulses of $\bar{n} = 0.1$, then Eve's knowledge $P_{B\wedge E}/P_B$ of Bob and Alice's common key will never be more than 2.5%. Thus, Alice and Bob have an upper bound on the amount of privacy amplification[25] needed to protect against a BS attack. Of course, such an attack would cause Bob's bit-rate to drop to near zero; for smaller reflection coefficients, R, Eve's information on Bob and Alice's key is reduced. For example, if Alice transmits pulses of $\bar{n} = 0.1$, and $R = T = 0.5$, then for every 250 key bits Alice and Bob acquire, Eve will know ~ 3 bits.

Conclusions

The results in this paper demonstrate free-space QKD through a turbulent medium under nighttime conditions. We have described a system that provides two parties a secure method to secretly communicate with a simple system based on the B92 protocol. This system was operated at a variety of average photon number per pulse down to an average of < 0.1 photon per pulse. The results were achieved with low BERs, and the 240-m experiment demonstrated that BERs of 0.7% or less are achievable with this system. This protocol could be implemented with classical signature authentication[2] and privacy amplification procedures to ensure the security of private information.

As a final discussion, we consider the feasibility to transmit the quantum states required in QKD between a ground station and a satellite in a low earth orbit. To that end, we designed our QKD system to operate at 772 nm where the atmospheric transmission from surface to space can be as high as 80%, and where single-photon detectors with efficiencies as high as 65% are commercially available; at these optical wavelengths atmospheric depolarizing effects are negligible, as is the amount of Faraday rotation experienced on a surface to satellite path.

To detect a single QKD photon it is necessary to know when it will arrive. The photon arrival time can be communicated to the receiver by using a bright precursor reference pulse. Received bright pulses allow the receiver to set a 1-ns time window

within which to look for the QKD photon. This short time window reduces background photon counts dramatically, and the background can be further reduced by using narrow bandwidth filters.

Atmospheric turbulence impacts the rate at which QKD photons would arrive at a satellite from a ground station transmitter. Assuming 30-cm diameter optics at both the transmitter and satellite receiver, the diffraction-limited spot size would be $\sim$ 1.2-m diameter at a 300-km altitude satellite. However, turbulence induced beam-wander can vary from $\sim 2.5-10$ arc-seconds leading to a photon collection efficiency at the satellite of $10^{-3}-10^{-4}$. Thus, with a laser pulse rate of 10 MHz, an average of one photon-per-pulse, and atmospheric transmission of $\sim$ 80%, photons would arrive at the collection optic at a rate of $800-10,000$ Hz. Then, with a 65% detector efficiency, the 25% intrinsic efficiency of the B92 protocol, IFs with transmission efficiencies of $\sim$ 70%, and a MM fiber collection efficiency of $\sim$ 40%, we find a key generation rate of $35-450$ Hz is feasible. With an adaptive beam tilt corrector the key rate could be increased by about a factor of 100 leading to a key rate of $3.5-45$ kHz; these rates will double using the BB84 protocol.

Errors would arise from background photons collected at the satellite. The nighttime earth radiance observed at 300 km altitude at the transmission wavelength is ~ 1 mW m^{-2} str^{-1} μm^{-1}, or $\sim 4 \times 10^{16}$ photons s^{-1} m^{-2} str^{-1} μm^{-1}, during a full moon, dropping to $\sim 10^{15}$ photons s^{-1} m^{-2} str^{-1} μm^{-1} during a new moon. Assuming a 5 arc-seconds receiver field of view, and 1-nm IFs preceding the detectors, a background rate of $\sim$ 800 Hz (full moon), and $\sim$ 20 Hz (new moon) would be observed (with a detector dark count rate of $\sim$ 50 Hz, the error rate will be dominated by background photons during full moon periods, and by detector noise during a new moon). We infer a BER from background photons of $\sim 9 \times 10^{-5}-10^{-3}$ (full moon), and $\sim 2 \times 10^{-6}-3 \times 10^{-5}$ (new moon).

During daytime orbits the background radiance would be much larger ($\sim 10^{22}$ photons s^{-1} m^{-2} str^{-1} μm^{-1}), leading to a BER of $\sim 2 \times 10^{-2}-3 \times 10^{-1}$, if an atomic vapor filter[26] of $\sim 10^{-3}$ nm bandwidth was used instead of the IF. (Note: it would also be possible to place the transmitter on the satellite. In this situation, the beam wander is similar, but it is only over the lowest $\sim$ 2 km of the atmosphere. In this situation, the bit-rate would improve by $\sim$ 150, decreasing the BER by the same amount.)

Because the optical influence of turbulence is dominated by the lowest $\sim$ 2 km of the atmosphere, our experimental results and this simple analysis show that QKD between a ground station and a low-earth orbit satellite should be possible on nighttime orbits and possibly even in full daylight. During the several minutes that a satellite would be in view of the ground station there would be adequate time to generate tens of thousands of raw key bits, from which a shorter error-free key stream of several thousand bits would be produced after error correction and privacy amplification. From these results we believe that it will be feasible to use free-space QKD for re-keying satellites in low-earth orbit from a ground station.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proc. of IEEE Int. Conf. on Comp., Sys., and Sig. Proc.*, Bangalore, India, p. 175 (1984).
2. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, New York (1997).
3. A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," Europhys. Lett. **23**, p. 383

(1993).
4. P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Enhanced single-photon fringe visibility in a 10 km-long prototype quantum cryptography channel," *Elec. Lett.* **29**, p. 634 (1993).
5. J. D. Franson and H. Ilves, "Quantum cryptography using optical fibers," *Appl. Opt.* **33**, p. 2949 (1994).
6. C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km," *Opt. Lett.* **20**, p. 1695 (1995).
7. R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, "Quantum cryptography," *Contemp. Phys.* **36**, p. 149 (1995).
8. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. M. Simmons, "Quantum cryptography over underground optical fibers," *Lecture Notes In Computer Science* **1109**, p. 329 (1996).
9. A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fiber," *Europhys. Lett.* **33**, p. 335 (1996).
10. R. J. Hughes, W. T. Buttler, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Secure communications using quantum cryptography," *Proc. of SPIE* **3076**, p. 2 (1997).
11. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Lecture Notes In Computer Science* **473**, p. 253 (1991).
12. W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Free-space quantum-key distribution," *Phys. Rev. A* **57**, p. 2379 (1998).
13. B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," *Opt. Lett.* **21**, p. 1854 (1996).
14. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Submitted to Phys. Rev. Lett.* (1998).
15. J. G. Walker, S. F. Seward, J. G. Rarity, and P. R. Tapster, "Range measurement photon by photon," *Quant. Opt.* **1**, p. 75 (1989).
16. S. F. Seward, P. R. Tapster, J. G. Walker, and J. G. Rarity, "Daylight demonstration of a low-light-level communication system using correlated photon pairs," *Quant. Opt.* **3**, p. 201 (1991).
17. C. A. Primmerman, D. V. Murphy, D. A. Page, B. G. Zollars, and H. T. Barclay, "Compensation of atmospheric optical distortion using a synthetic beacon," *Nature (London)* **353**, p. 141 (1991).
18. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.* **68**, p. 3121 (1992).
19. J. F. Clauser, "Experimental distinction between quantum and classical field-theoretic predictions for photoelectric effect," *Phys. Rev. D* **9**, p. 853 (1974).
20. W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned," *Nature (London)* **299**, p. 802 (1982).
21. A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on quantum cryptosystems," *Phys. Rev. A* **50**, p. 1047 (1994).
22. B. E. A. Saleh and M. C. Teich, "Fundamentals of Photonics," Jon Wiley and Sons, Inc., New York (1991).
23. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Free-space quantum key distribution at night," *Proc. of SPIE* **3385**, p. 14 (1998).
24. P. D. Townsend, "Quantum Cryptography over multi-user optical fibre networks," *Nature (London)* **385**, p. 47 (1997).
25. C. H. Bennett, G. Brassard, C. Crepeau, C., and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Th.* **41** p. 1915 (1995).
26. H. Zhilin, X. Sun, and X. Zeng, "Rb 780 nm Faraday anomalous dispersion optical filter in a strong magnetic field," *Opt. Communications* **101**, p. 175 (1993).