LA-UR- 99-130

CONF-990110--

Approved for public release; distribution is unlimited.

Title: Quantum cryptography for secure free-space communications

Author(s): Richard J. Hughes, William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux, Gabriel G. Luther, George L. Morgan, Jane E. Nordholt and C. Glen Peterson

Submitted to: Proceedings of SPIE "Photonics West" conference, San Jose, CA 23-29 January, 1999

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Quantum cryptography for secure free-space communications

Richard J. Hughes,* William T. Buttler, Paul G. Kwiat, Steve K. Lamoreaux, Gabriel G. Luther, George L. Morgan, Jane E. Nordholt and C. Glen Peterson

University of California, Los Alamos National Laboratory, Los Alamos, NM 87545

ABSTRACT

The secure distribution of the secret random bit sequences known as "key" material, is an essential precursor to their use for the encryption and decryption of confidential communications. Quantum cryptography is a new technique for secure key distribution with single-photon transmissions: Heisenberg's uncertainty principle ensures that an adversary can neither successfully tap the key transmissions, nor evade detection (eavesdropping raises the key error rate above a threshold value). We have developed experimental quantum cryptography systems based on the transmission of non-orthogonal photon polarization states to generate shared key material over line-of-sight optical links. Key material is built up using the transmission of a single-photon per bit of an initial secret random sequence. A quantum-mechanically random subset of this sequence is identified, becoming the key material after a data reconciliation stage with the sender. We have developed and tested a free-space quantum key distribution (QKD) system over an outdoor optical path of ~1 km at Los Alamos National Laboratory under nighttime conditions. Results show that free-space QKD can provide secure real-time key distribution between parties who have a need to communicate secretly. Finally, we examine the feasibility of surface to satellite QKD.

Keywords: Cryptography; Optical Communications; Quantum Information

1. QUANTUM CRYPTOGRAPHY: INTRODUCTION

Two of the main goals of cryptography are the encryption of messages to render them unintelligible to third parties and their authentication to certify that they have not been modified. These goals can be accomplished if the sender ("Alice") and recipient ("Bob") both possess a secret random bit sequence known as "key" material, which they use as a parameter in a cryptographic algorithm. It is essential that Alice and Bob acquire the key material with a high level of confidence that any third party ("Eve") does not have even partial information about the random bit sequence. If Alice and Bob communicate solely through classical messages it is impossible for them to generate a certifiably secret key owing to the possibility of passive eavesdropping. However, secure key distribution becomes possible if they use the single-photon communication technique of quantum cryptography, or more accurately, quantum key distribution (QKD),[1] which was introduced in the mid-1980s. 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, or from the physical security of the distribution process.

Since the introduction of quantum cryptography, several groups (including our own) have demonstrated quantum communications[2, 3] and key distribution[4, 5, 6, 7, 8, 9] over multi-kilometer distances of optical fiber. Free-space QKD (over an optical path of 32 cm) was first introduced in 1991,[10] and recent advances have led to demonstrations of QKD over free-space indoor optical paths of 205 m,[11] and outdoor optical paths of 75 m.[12] These demonstrations increase the utility of QKD by extending it to line-of-site optical 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). We are developing both optical fiber and free-space QKD prototypes, and here we report our results of free-space QKD over outdoor optical paths of up to 950 m under nighttime conditions.[13]

The success of QKD over free-space optical paths depends on the transmission and detection of single optical photons against a high background through a turbulent medium. Although this problem is difficult, a combination of sub-nanosecond timing, narrow filters[14, 15], spatial filtering[11] and adaptive optics[16] can render the transmission and detection problems tractable. Furthermore, the essentially non-birefringent nature of the atmosphere at optical wavelengths allows the faithful transmission of the single-photon polarization states used in the free-space QKD protocol.

*Correspondence: email: hughes@lanl.gov; WWW: http://p23.lanl.gov/Quantum/quantum.html

2. QUANTUM CRYPTOGRAPHY: THEORY

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[17] Alice agrees with Bob (through public discussion) that she will transmit a horizontally-polarized single-photon state, |H>, for each "0" in her sequence, and a right-circularly-polarized single-photon state, |R>, for each "1" in her sequence. Bob agrees with Alice to randomly test the polarization of each arriving photon for vertical polarization, |V>, to reveal "1s," or left-circular polarization, |L>, 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> and |V>, which happens for 50% of the bits in Alice's sequence. However, for the other 50% of Alice's bits the preparations and measurements use non-identical states, such as |H> and |L>, resulting in a random 50% detection probability for Bob on this portion. Thus, by detecting single photons Bob identifies a random 25% portion of the bits in Alice's random sequence, assuming she transmits a single-photon Fock state for each bit and there are no bit losses 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 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,[18] nor copy them, owing to the quantum "no-cloning" theorem.[19] 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."[20]

3. FREE-SPACE QUANTUM CRYPTOGRAPHY EXPERIMENT

The QKD transmitter in our experiment (see figure 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 27x beam expander. The diode laser wavelength is temperature adjusted to 772 nm, and the laser is configured to emit a short pulse of approximately 1-ns length, containing $\sim 10^5$ photons.

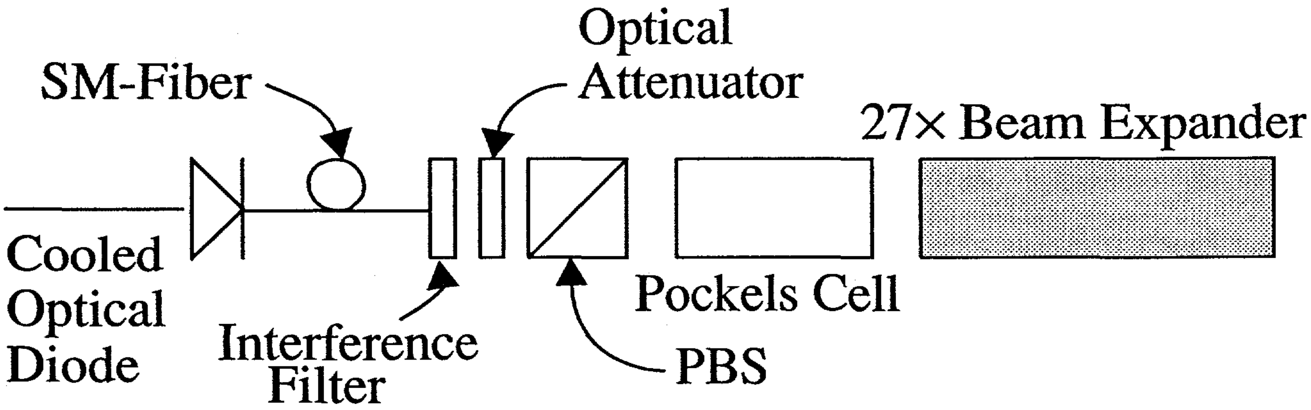

Figure 1. Free-space QKD transmitter (Alice).

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 ~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. (The attenuated pulse only approximates a "single-photon" state; we tested out the system with averages down to < 0.1 photons 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.) The photons that are transmitted by the optical attenuator are then polarized by the PBS, which transmits an average of less than one |H> photon to the Pockels cell. The

Pockels cell is randomly switched to either pass the light unchanged as |H> (zero-wave retardation) or change it to |R> (quarter-wave retardation). The random switch setting is determined by discriminating the voltage generated by a white noise source.

The QKD receiver (see figure 2) was comprised of 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) followed by a PBS to test collected photons for |H>; the upper optical path contained a half-wave retarder followed by a PBS to test for |R>. One 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 (~1.1 kHz) to negligible levels.]

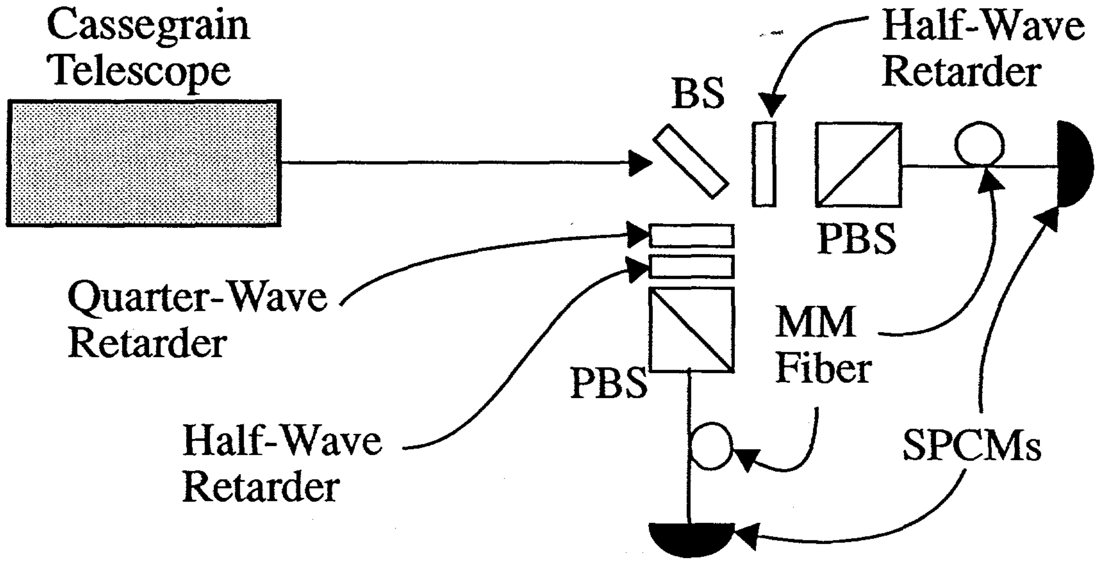

Figure 2. Free-space QKD receiver (Bob).

A single |R> photon traveling along the lower path encounters the polarization controller, and is converted to |V> and reflected away from the SPCM. Conversely, a single |H> photon traveling the same path is converted to |R> and transmitted toward or reflected away from the SPCM in this path with equal probability. Similarly, a single |H> photon traveling the upper path is converted to |V> and reflected away from the SPCM in this path, but a single |R> photon traveling this path is converted to |L> and transmitted toward or reflected away from the SPCM with equal probability.

The transmitter and receiver optics were operated over 240-, 500-, and 950-m outdoor optical paths under nighttime conditions, with the transmitter and receiver co-located in order to simplify data acquisition. All optical paths were achieved by reflecting the emitted beam from a 25.4-cm mirror positioned at the half-way point of the transmission distance.

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

$$P_B = e^{-\bar{n}} \sum_{n=1}^{\infty} \frac{\bar{n}^n}{n!}\left[1-y^n\right] = 1-e^{-\bar{n}\eta_B} \qquad (1)$$

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 $\eta_B = \eta \times \eta_D \times \eta_Q$, 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 photons per pulse for the 950-m path, Eq. (1) gives $\bar{n} \times \eta_B = 0.1 \times (0.14 \times 0.25 \times 0.65) \sim 2.3 \times 10^{-3}$, 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 ~ 1.5 % when the system was operating down to the < 0.1 photons per pulse level. (A BER of ~ 0.7 % was observed over the 240-m optical path and a BER of ~ 1.5 % was also observed over the 500-m optical path.) A sample of raw key material from the 950-m experiment, with errors marked in bold type, is shown below:

a 10010010100010000011000001011100001111111111000000
b 100100101000100000110000010111000011111111**0**1000000

a 10101011011111100111111011110101001101001011101111
b 10101011011111100**0**11111011110101001101001011101111

A 100-bit sample of Alice's (a) and Bob's (b) raw key material generated by free-space QKD over 1 km.

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).

This experiment implemented a two-dimensional parity check scheme that allowed the generation of error-free key material. A further stage of "privacy amplification"[21] is necessary to reduce any partial knowledge gained by an eavesdropper to less than 1-bit of information; we have not implemented such a privacy amplification protocol at this time. Our free-space QKD system does incorporate "one time pad" encryption[22]--- the only provably secure encryption method---and could also support any other symmetric key system.

4. EAVESDROPPING ATTACKS

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]

$$P_{B\wedge E} = \left[1 - e^{-\bar{n}\eta_E R}\right] \cdot \left[1 - e^{-\bar{n}\eta_B T}\right] \qquad (2)$$

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 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.

5. QUANTUM CRYPTOGRAPHY FOR SECURE SATELLITE COMUNICATIONS

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 ~1.2-m diameter at a 300-km altitude satellite. However, turbulence induced beam-wander can vary from ~ 2.5 to 10 arc-seconds leading to a photon collection efficiency at the satellite of 10^{-3} to 10^{-4}. Thus, with a laser pulse rate of 10 MHz, an average of one photon-per-pulse, and atmospheric transmission of ~ 80%, photons would arrive at the collection optic at a rate of 800 to 10,000 Hz. Then, with a 65% detector efficiency, the 25% intrinsic efficiency of the B92 protocol, IFs with transmission efficiencies of ~ 70%, and a MM fiber collection efficiency of ~ 40%, we find a key generation rate of 35 to 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 to 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 ~ 4 x 10^{16} photons s^{-1} m^{-2} str^{-1} μm^{-1}, during a full moon, dropping to ~ 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 ~ 800 Hz (full moon), and ~ 20 Hz (new moon) would be observed (with a detector dark count rate of ~ 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 ~ 9 x 10^{-5} to 10^{-3} (full moon), and ~ 2 x 10^{-6} to 3 x 10^{-5} (new moon).

During daytime orbits the background radiance would be much larger (~ 10^{22} photons s^{-1} m^{-2} str^{-1} μm^{-1}), leading to a BER of ~ 2 x 10^{-2} to 3 x 10^{-1}, if an atomic vapor filter[25] of ~ 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 because it is only over the lowest ~ 2 km of the atmosphere the bit-rate would improve by ~ 150, decreasing the BER by the same amount.)

Because the optical influence of turbulence is dominated by the lowest ~ 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.

6. SUMMARY AND CONCLUSIONS

This paper demonstrates practical free-space QKD over 1-km 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. We presented two attacks on this protocol and demonstrated the protocol's built-in protections against them. This system was operated at a variety of average photon numbers per pulse down to $\bar{n} < 0.1$. 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. We have recently constructed a point-to-point free-space QKD system and operated it with low BERs over a 0.5-km outdoor optical path in daylight. From these results and those presented here 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, *Proc. of IEEE Int. Conf. on Comp., Sys., and Sig. Proc.*, Bangalore, India, (IEEE, New York, 1984) p.175.
2. A. Muller, J. Breguet, and N. Gisin, *Europhys. Lett.* **23**, 383 (1993).
3. P. D. Townsend, J. G. Rarity, and P. R. Tapster, *Elec. Lett.* **29**, 634 (1993).
4. J. D. Franson, and H. Ilves, *Appl. Opt.* **33**, 2949 (1994).
5. C. Marand, and P. D. Townsend, *Opt. Lett.* **20**, 1695 (1995).
6. R. J. Hughes et al., *Contemp. Phys.* **36**, 149 (1995).
7. R. J. Hughes et al., *Lecture Notes In Computer Science* **1109**, 329 (1996).
8. A. Muller, H. Zbinden, and N. Gisin, *Europhys. Lett.* **33**, 335 (1996).
9. R. J. Hughes et al., *Proc. SPIE* **3076**, 2 (1997).
10. C. H. Bennett et al., *Lecture Notes In Computer Science* **473**, 253 (1991).
11. W. T. Buttler et al., *Phys. Rev. A* **57**, 2379 (1998).
12. B. C. Jacobs, and J. D. Franson, *Opt. Lett.* **21**, 1854 (1996).
13. W. T. Buttler et al., *Phys. Rev. Lett.* **81**, 3283 (1998).
14. J. G. Walker et al., *Quant. Opt.* **1**, 75 (1989).
15. S. F. Seward et al., *Quant. Opt.* **3**, 201 (1991).
16. C. A. Primmerman et al., *Nature* **353**, 141 (1991).
17. C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
18. J. F. Clauser, *Phys. Rev. D* **9**, 853 (1974).
19. W. K. Wooters, and W. H. Zurek, *Nature* **299**, 802 (1982).
20. A. K. Ekert et al., *Phys. Rev. A* **50**, 1047 (1994).
21. C. H. Bennett et al., *IEEE Trans. Inf. Th.* **41**, 1915 (1995).
22. G. S. Vernam, *Trans. Am. Inst. Elect. Eng.* **XLV**, 295 (1926).
23. W. T. Buttler et al., *Proc. SPIE* **3385**, 14 (1998)
24. P. D. Townsend, *Nature* **385**, 47 (1997).
25. H. Zhilin, X. Sun, and X. Zeng, *Opt. Communications* **101**, 175 (1993).