LA-UR- 98-1177

Approved for public release; distribution is unlimited.

Title: FREE-SPACE QUANTUM KEY DISTRIBUTION AT NIGHT

CONF-980412 --

Author(s):
W. T. Buttler, P-23
R. J. Hughes, P-23
P. G. Kwiat, P-23
S. K. Lamoreaux, P-23
G. L. Morgan, P-23
C. G. Peterson, P-23
C. M. Simmons, P-23
G. G. Luther, P-22
J. E. Nordholt, NIS-1

Submitted to: AEROSENSE '98, SPIE PROCEEDINGS, ORLANDO, FL, APRIL 13-14, 1998

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

DISCLAIMER

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

Free-space quantum key distribution at night

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

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; in this paper, 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, and the effectiveness of privacy amplification procedures is discussed. Our conclusions are that free-space QKD is both effective and secure; possible applications include the rekeying of satellites in low earth orbit.

Keywords: Cryptography, Quantum Cryptography, Quantum Key Distribution, Eavesdropping, Parity Check, Privacy Amplification, Bennett 92, Error Detection, Information Security, Satellite

1. 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 distribution process.

Since the introduction of quantum cryptography, several groups have demonstrated quantum key distribution (QKD) over multi-kilometer distances of optical fiber,[3-10] 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 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). We are developing QKD for use over line-of-sight paths, and here we report our results of free-space QKD key generation over outdoor optical paths of up to 950 m under nighttime conditions.

2. QUANTUM KEY DISTRIBUTION

The success of QKD over free-space optical paths depends on the transmission of single-photons through a turbulent medium and their detection against a high background. Although this problem is difficult, a combination of sub-nanosecond timing, narrow filters,[13,14] spatial filtering[11] and adaptive optics[15] 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.

Send correspondence to W. T. Buttler: E-mail: buttler@lanl.gov

Table 1. Observation Probabilities

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

2.1. 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[16] 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 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,[17] nor copy them, owing to the quantum "no-cloning" theorem.[18] 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.[19]"

2.2. QUANTUM-KEY TRANSMITTER: ALICE

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

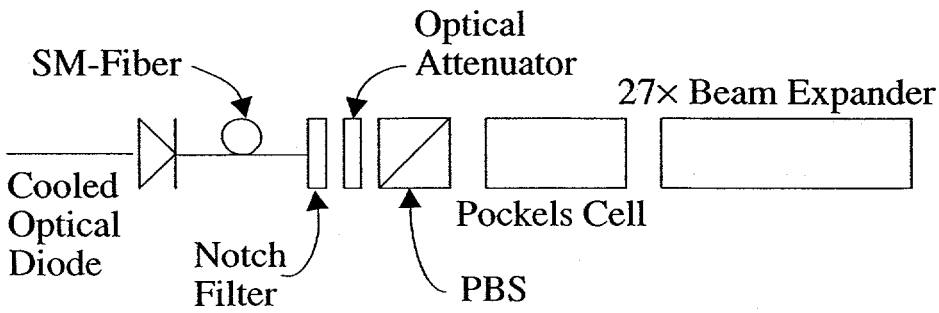

Figure 1. QKD Transmitter.

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 notch filter, 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. (The attenuated pulse only approximates a "single-photon" state; we tested the system with averages of 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, $P^{\bar{n}}$, 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.

2.3. 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 $|h\rangle$; 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 notch filters, 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, 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; however, 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 $|r\rangle$ photon traveling this path is converted to $|\ell\rangle$ and transmitted toward or reflected away from the SPCM with equal probability.

*A polarization controller was not required along the upper path because the 50/50 BS transmitted the P polarization without introducing any phase shift, but the quarter- and half-wave retarder pair was necessary along the lower path because the BS reflected the S and P polarizations differently, introducing some ellipticity to the reflected wave.

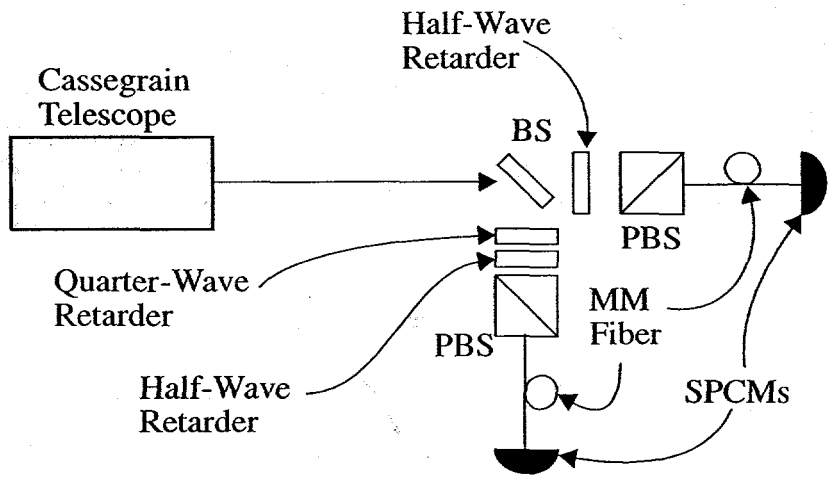

Figure 2. QKD receiver.

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. However, while the remaining two paths contain indeterminate polarization information, this information is important for the secure implementation of B92, as will be seen later (see Sec 4.1).

3. 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 locating 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.

3.1. SYSTEM EFFICIENCY

In determining Bob's bit-rate, we consider that a BS partitions a coherent photon stream in a binomial fashion. We further assume that the effective wave retarders, combined with the PBSs, behave together as 50/50 BSs when analyzing non-orthogonal polarizations, i.e, $|h\rangle$ and $|\ell\rangle$, and $|r\rangle$ and $|v\rangle$. In addition, we treat the detectors as BSs with transmission coefficient $T = 0.65$, or in other words, that the detector with efficiency $\eta_D = 0.65$ also partitions coherent photon streams in a binomial way; we also treat the transmission and reception efficiency η, or power losses between the transmitter and receiver, and the losses which occur coupling power into the receiver's MM fibers, as random binomial processes. The binomial probability distribution is summarized in Eq. 1.

$$p_{\geq 1}^{n} = \sum_{m=1}^{n} \binom{n}{m} \cdot T^{m} \cdot R^{n-m} . \tag{1}$$

This equation gives the probability that at least 1 photon, from a coherent photon stream of n photons, will be transmitted through the optical elements along the optical path the photon stream is traveling. The transmission probability is T, the reflection probability is R, and $T + R = 1$.

For calculation purposes, we use Eq. 2, which is equivalent to Eq. 1.

$$p_{\geq 1}^{n} \equiv 1 - (1 - \eta \cdot \eta_D \cdot 1/2 \cdot 1/2)^{n} , \tag{2}$$

where η, and η_D, are as previously defined, and the factor of $1/4 = 1/2 \cdot 1/2$, gives the transmission probability through the first 50/50 BS followed by either effective wave retarder and PBS pair—given the appropriate polarization.

These binomial expanded products (Eq. 2) of η, 1/4, and η_D, are convolved with the Poisson probabilities that there will be exactly n photons in a pulse given that the average number of photons per pulse is $\bar{n}$. The Poisson probability, $P_n^{\bar{n}}$, is shown in Eq. 3.

$$P_n^{\bar{n}} = \frac{\bar{n}^{n} \cdot \exp(-\bar{n})}{n!} . \tag{3}$$

The convolution is summed to give the detection probability as a function of the Poisson average photon number. This probability multiplied by the rate at which Alice transmits the coherent pulses, R_A, gives the rate at which Bob detects 0s and 1s, R_B. Our experimental result was $R_B \sim 50$ Hz when the transmitter was pulsed at a rate of $R_A = 20$ kHz, with $\bar{n} = 0.1$ photon per pulse for the 950-m path. This result is expressed in Eq. 4.

$$R_B = R_A \sum_{n=1}^{\infty} [1 - (1 - \eta \cdot \eta_D/4)^{n}] \cdot \frac{\bar{n}^{n} \exp(-\bar{n})}{n!} . \tag{4}$$

Finally, we note that in the limit that $\eta \cdot \eta_D \mapsto 1$, and given a Fock state of $m \equiv 1$ photon, then $\bar{n} \mapsto 1$ and the Poisson probability distribution $P^{\bar{n}} \mapsto \delta_{m-1}$, i.e., $\delta_{m-1} = 0 \,\forall\, m \neq 1$. In this limit—the limit of a perfect, lossless system—the sum vanishes and we are left with exactly 1 term which shows that Bob and Alice sacrifice 75% of their bits for privacy.

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

3.2. SYSTEM INEFFICIENCY

The bit error rate (BER) for the 950 m path was $\sim 1.5\%$ when the system was operating down to the < 0.1 photon per pulse level, where the BER is defined as the ratio of the bits received in error to the total number of bits received. A BER of $\sim 0.7\%$ 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, is shown in Table 2.

Bit errors caused by the ambient background ($\sim$ 1.1 kHz) were minimized to less than $\sim$ 1 every 9 s by the narrow gated coincidence timing windows ($\sim$ 5 ns) and the spatial filtering. Further, because detector dark noise ($\sim$ 80 Hz) contributed only about 1 dark count every 125 s, we believe that the BER was caused by misalignment and imperfections in the optical elements (wave-plates and Pockels cell).

3.3. 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 (see Sec. 2.1) into 2D arrays 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 further ensure privacy, Alice and Bob also discard the bits oriented along the diagonals. This guarantees the elimination of two bits for each row and column of the matrix, even when no errors are detected, and frustrates knowledge revealed during the parity exchange.[†]

Figure 3 illustrates the error detection protocol. In this example, Alice possesses the 'good' bits, and it is necessary for her and Bob to remove his 'bad' bits and distill error free key material. Bob possesses only two bad bits, but after openly communicating the column and row parities, they sacrifice good bits along the diagonals, and the 2 rows and 2 columns where parity differences were seen (parity differences are seen in columns 3 and 6 and rows 3 and 6). The net result, in this example, is 24 error-free bits: $key := \{100000110111110000010111\}$. Thus, in addition to the minimum 75% key lost during the B92 protocol, Bob and Alice have sacrificed another 62.5% of the detected bits.

This is not the whole story, because the detection protocol does not detect all errors. For example, 2 errors in a column, combined with another error in a row containing one of the column errors (an 'L' shaped pattern), results in a missed bit-error. If there were 4 errors in a 'box' pattern, none of the errors would be detected, and so on.

We must emphasize, however, the strengths of the 2D routine as well. For example, the minimum Hamming distance,[20] d, for a 2D scheme is the square of the minimum Hamming distance of the same detection scheme implemented in one-dimension (1D). (The Hamming distance tells how many errors can be detected, and/or corrected—one can detect $d-1$ errors.) For our particular detection code, a parity check code, the minimum Hamming distance is 2 for the 1D case, but in 2D this becomes 4. Once again, this is not the whole story, because there are situations in the 1D parity check scheme where more than one error can be detected, if the word is long enough; parity in 1D can detect an odd number of bit flips: 1, 3, 5, etc; however, even parity flips cannot be detected.[‡]

[†]To ensure the security of the error detection protocol, and to simplify it, we implement the algorithm for square matrices of an even dimension.

[‡]We make no attempt to correct for errors, and comment that cyclic redundancy codes are more powerful than the parity codes. For our specific application, the parity check code allows us to keep more key material while maintaining the capability to frustrate Eve.

To test our error detection scheme, we simulated random 0's and 1's with errors and found that key material with bit errors had to be processed with the detection protocol several times to reduce errors to negligible levels. On the first error pass, small 2D matrices were needed (for key with high BERs), but with each subsequent detection pass, a larger 2D matrix could be used. We found that data with BERs as high as 10% could be reduced to an estimated ~ 1 bit-error in a total of 10^9 bits after 4 passes, with $\sim 14\%$ of the initial key remaining; the sizes of the matrices in the 4 passes were 6 by 6, 7 by 7, 13 by 13, and 13 by 13, respectively. (We never operated our system with BERs this high, but in our simulations we wanted to determine the detection scheme's capabilities. We also found that there exists an optimal matrix size which most efficiently reduced errors while preserving a maximal amount of key material. The sizes varied from a 6 by 6 to a 12 by 12, almost linearly, for BERs between 10% and 1%.)

Finally we note that because Alice transmits coherent states, as opposed to single photon Fock states, she and Bob also need to add a stage of "privacy amplification[21]" 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, but our free-space QKD system does incorporate "one time pad"[22] encryption—also known as the Vernam Cipher: the only provably secure encryption method—and could also support any other symmetric key system.

4. EAVESDROPPING: AN ATTACK BY EVE

Much has been said about the security of QKD against attack by an eavesdropper.[19] In fact, B92 is not provably secure. There are essentially two types of attack to consider: opaque attacks and translucent attacks.

4.1. OPAQUE ATTACK

In an opaque attack, often referred to as the "man in the middle," Eve intercepts all collectable bits, or single photons, by positioning herself between Alice and Bob. If Eve possesses a transmitter and receiver identical in every way to Bob's receiver and Alice's transmitter, and Bob, Alice and Eve are operating under the B92 protocol, then Eve can determine as much information about the key as could Bob. For example, if Alice's transmission basis is $|h\rangle$ and $|r\rangle$, and Eve's measurement basis is $|\ell\rangle$ and $|v\rangle$, then Eve can know Alice's transmitted bits with a maximum efficiency of 25%.[§] If Eve retransmits the bits she "knows," then she will lower Bob's expected bit-rate, relative to Alice, by at least a factor of 4, but she will be forwarding bits of the correct value to Bob.

If Eve can collect, measure, and quickly retransmit the bits she detects, then she can then listen to Alice's and Bob's open bit reconciliation protocol (see Sec. 2.1). And, while Bob never reveals his bits values, Eve still knows

[§]In a real system, Eve will experience reception losses associated with the collection, fiber launch and detection of the single photons. In addition, there will be bit-errors associated with the transmission and measurement protocols, i.e., impure bit preparation and measurement associated with optical alignment of the transmission, receiving, and analysis optics.

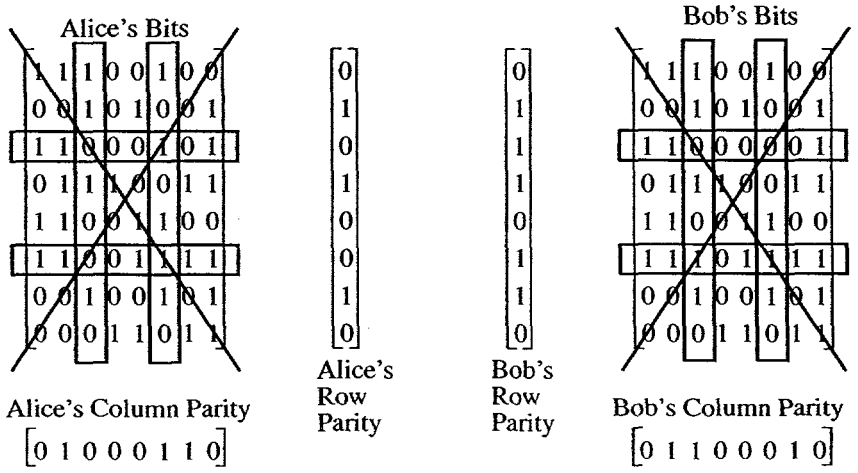

Figure 3. Two-dimensional parity check scheme.

what bits Alice and Bob commonly share because she possesses the timing information about Alice's initial reference pulse. At this point, if Alice and Bob know their system well, Eve has been revealed by the additional factor of 4 attenuation, e.g., Eve has discarded a minimum of 75% of her bits, but Alice has discarded a minimum of 93.75% of her bits.

Some could argue this additional attenuation to Bob's and Alice's common key is protection enough against an opaque attack, but our implementation of B92 adds another layer of protection if Eve attempts to bring Bob's bit rate to a rate indistinguishable from her own. Eve can do this by retransmitting a bright classical pulse to Bob for each single photon she detects.[¶] However, our system protects against this attack when operated in either a 2, 3, or 4 SPCM mode. In a 2 SPCM system, this type of attack would be revealed through an increase in "dual-fire" errors. (Dual-fire errors occur when both SPCMs fire simultaneously. In a perfect system there would be no dual-fire errors, regardless of the average photon number per pulse, but in an imperfect experimental system, where bit-errors occur, dual-fire errors will occur.)

If we consider only a perfect system, then no matter how many horizontally polarized photons travel the $|r\rangle$ analysis path, none will reach the $|r\rangle$ analyzing detector. However, if this analysis path includes an effective half-wave retarder followed by a PBS, then the half wave-retarder will convert right-circular polarized photons to left-circular polarized photons which will then be equally split equally between the two output paths. If both paths then are each followed by an SPCM, then both SPCMs will fire.

The half of a right-circular polarized pulse which travels the $|h\rangle$ analysis path encounters the effective quarter-wave retarder followed by another PBS. The quarter-wave retarder converts this right-circular polarized 'bright' pulse to a vertical-polarized 'bright' pulse which is reflected along the path away from the $|h\rangle$ analyzing detector. If this path contains an SPCM, then this SPCM will fire together with the two SPCMs which terminate on the $|r\rangle$ analyzing path.Thus, 3 of 4 detectors have fired alerting Bob and Alice that Eve is opaquely attacking the key. A similar argument applies if Bob is using 3 detectors.

4.2. TRANSLUCENT ATTACK

Eve could also passively, or translucently, attack the key with a BS. In this scheme, Eve gets the binomial expansion of the BS she uses to reflect key material her way, and Bob gets the binomial expansion of what is transmitted. It is necessary to consider Eve's and Bob's efficiencies, which are independent of the other. Equation 5 shows the amount of information on the key Eve gets as a function of the reflection coefficient, $R = 1 - T$, of her BS, and Eq. 6 shows the amount of key Bob gets as a function of the transmission coefficient, T, of her BS.

$$R_E = R_A \sum_{n=1}^{\infty} [1 - (1 - \frac{\eta_E \cdot \eta_D^E \cdot (1-T)}{4})^n] \cdot \frac{\bar{n}^n \exp(-\bar{n})}{n!}, \tag{5}$$

and

$$R_B = R_A \sum_{n=1}^{\infty} [1 - (1 - \frac{\eta_B \cdot \eta_D^B \cdot T}{4})^n] \cdot \frac{\bar{n}^n \exp(-\bar{n})}{n!}, \tag{6}$$

where η_B accounts for losses between the transmitter and the power Bob could couple into the MM fibers at his receiver, if Eve's BS were 100% transmissive, and η_E accounts for losses between the transmitter and the power Eve could couple into the MM fibers at her receiver if her BS was 100% reflective. Eve's and Bob's detector efficiencies are, respectively, η_D^E, and η_D^B. The 1/4 reduction of these products is as previously described in Sec 3. Eve's bit rate is R_E, and R_B is Bob's, and R_A is the rate Alice is transmitting.

The privacy, or the amount of information Eve possesses on Alice's and Bob's common key takes a bit more work to extract. We first must determine how many bits Eve and Bob observe coincidently, because only those bits which both she and Bob possess are of any use to her. First of all, if there is only 1 bit in a pulse, then either Eve or Bob will get it, but not both. Based on this premise, Eq. 7 shows the number of bits that Bob and Eve will share (observe coincidently) if Eve attacks the key with a BS of transmission coefficient T, and reflection coefficient $R = 1 - T$.

$$N_{B \wedge E} = R_A \sum_{n=2}^{\infty} \frac{\bar{n}^n \exp(-\bar{n})}{n!} \sum_{m=1}^{n-1} \binom{n}{m} \cdot T^m \cdot R^{n-m} \cdot [1 - (1 - \frac{\eta_B \cdot \eta_D^B}{4})^m] \cdot [1 - (1 - \frac{\eta_E \cdot \eta_D^E}{4})^m]. \tag{7}$$

[¶]In B92 it is possible to send coherent classical pulses of the approriate polarization and insure that every bit transmitted is detected at the receiver.

Equation 8 shows Alice's and Bob's privacy, P.

$$P = \frac{\sum_{n=2}^{\infty} \frac{\bar{n}^n \exp(-\bar{n})}{n!} \sum_{m=1}^{n-1} \binom{n}{m} \cdot T^m \cdot R^{n-m} \cdot [1-(1-\frac{\eta_B \cdot \eta_D^B}{4})^m] \cdot [1-(1-\frac{\eta_E \cdot \eta_D^E}{4})^{n-m}]}{\sum_{n=1}^{\infty} [1-(1-\frac{\eta \cdot \eta_D \cdot T}{4})^n] \cdot \frac{\bar{n}^n \exp(-\bar{n})}{n!}}. \quad (8)$$

Under this type of translucent attack, if Eve uses 50/50 BS, and if Alice transmits coherent Poisson pulses with an average of 0.1 photon per pulse, then for every ~ 250 bits Eve and Bob acquire, Eve will commonly share ~ 3 of her 250 bits with Bob's 250 bits (or $\sim 3/250$ of Alice and Bob's common key—this estimate assumes perfect system efficiencies for both Bob and Eve). Eve's knowledge on Alice's and Bob's common key is coupled to her own system efficiencies and drops dramatically under experimental conditions where collection and detection efficiencies are imperfect.

Eve could determine which bits she commonly shares with Bob when Alice and Bob reconcile their common bits, but her bit knowledge would be reduced during the error detection procedure Alice and Bob perform. However, seldom would her information be completely destroyed during this step of bit reconciliation, but Bob and Alice can easily reduce Eve's knowledge to less than 1-bit of information by performing a classical privacy amplification procedure on their common key, if they know the maximum information Eve could have.

5. CONCLUSIONS

This paper demonstrates 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. 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 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. 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.

ACKNOWLEDGMENTS

R. J. H. wishes to extend special thanks to J. G. Rarity for the many helpful discussions regarding free-space quantum cryptography, and W. T. B. extends his appreciation to A. G. White for helpful discussions regarding QKD, and to Doug Fulton for use of the streak camera and spectrograph for optical diagnostics.

REFERENCES

1. C. H. Bennett, and G. Brassard, Proc. of IEEE Int. Conf. on Comp., Sys., and Sig. Proc., Bangalore, India, 175 (1984).
2. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of App. Cryptography, CRC Press (1997).
3. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
4. A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).
5. P. D. Townsend, J. G. Rarity, and P. R. Tapster, Elec. Lett. **29**, 634 (1993).
6. C. Marand, and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
7. J. D. Franson, and H. Ilves, Appl. Opt. **33**, 2949 (1994).
8. R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Contemp. Phys. **36**, 149 (1995).
9. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, Lecture Notes In Computer Science **1109**, 329 (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, Proc. of SPIE **3076**, 2 (1997).

11. 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, Tentatively Scheduled For: Phys. Rev. A **57** (1998).
12. B. C. Jacobs, and J. D. Franson, Opt. Lett. **21**, 1854 (1996).
13. J. G. Walker, S. F. Seward, J. G. Rarity, and P. R. Tapster, Quant. Opt. **1**, 75 (1989).
14. S. F. Seward, P. R. Tapster, J. G. Walker, and J. G. Rarity, Quant. Opt. **3**, 201 (1991).
15. C. A. Primmerman, D. V. Murphy, D. A. Page, B. G. Zollars, and H. T. Barclay, Nature (London) **353**, 141 (1991).
16. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
17. J. F. Clauser, Phys. Rev. D **9**, 853 (1974).
18. W. K. Wooters, and W. H. Zurek, Nature (London) **299**, 802 (1982).
19. A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
20. R. W. Hamming, Coding and Information Theory, Prentice Hall, New Jersey (1980).
21. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Th. **41**, 1915 (1995).
22. G. S. Vernam, Trans. Am. Inst. Electr. Eng. **XLV**, 295 (1926).