LA-UR- 98-1272

*Approved for public release; distribution is unlimited.*

Title:

# PRACTICAL FREE-SPACE QUANTUM CRYPTOGRAPHY

CONF-980245--

Author(s):

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

Submitted to:

Lecture Notes in Computer Science, 1st NASA QC QC Conference

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.

# Practical free-space quantum cryptography

R. J. Hughes, W. T. Buttler, 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
hughes@lanl.gov
WWW home page: http://p23.lanl.gov/Quantum/quantum.html

**Abstract.** An experimental free-space quantum key distribution (QKD) system has been tested over an outdoor optical path of ~ 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, 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.

## 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 quantum key generation over outdoor optical paths of up to 950 m under nighttime conditions.

## 2 Quantum-Key Distribution

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 subnanosecond timing techniques, narrow wavelength filters [13, 14] spatial filtering [11], and adaptive optics [15]. To define the problem, we will require the generation of $\sim 1,000$ secret key bits between a ground station and a low-earth orbit satellite ($\sim$ 300 km altitude) in one overhead pass (duration $\sim$ 8 minutes). In the following analysis we will assume that the QKD transmitter (Alice) is at the ground station and the receiver is on the satellite (Bob).

### 2.1 Free-Space Single Photon Detection and Transmission

The operational wavelength for free-space QKD should be chosen for both good atmospheric transmission properties and high detection efficiency. We have chosen to work at 772 nm where the atmospheric transmission from surface to space can be as high as 80% and single-photon detectors with efficiencies as high as 65% are commercially available (silicon avalanche photodiodes: APDs). Furthermore, at these optical wavelengths depolarizing effects of atmospheric turbulence are negligible as is the amount of Faraday rotation experienced on a surface to satellite path.

In order to detect a single QKD photon it is necessary to know when it will arrive. However, there will be variations in transmission time through the atmosphere owing to turbulence induced variations in refractive index, with time scales of the order of $0.01 - 0.1$ s. Therefore, the photon arrival time can be communicated to the receiver by using a bright (multi-photon) precursor reference pulse, transmitted 100 ns (say) ahead of each QKD photon. The bright pulse and the "single photon" (produced by highly attenuating the pulsed output of a semiconductor laser) would each be of a $\sim$ 100-ps duration. (Note: the temporal length of the bright pulse is not as restricted as the temporal length of the dim-pulse; in fact, the bright pulse only needs to be short enough to allow the detection of the bright- and dim-pulses within the time allowed by the transmission rate. We also note that the atmosphere is only weakly dispersive.) The received bright pulse would then allow the receiver to set a 1-ns time window (say) within which to look for the QKD photon. This short time window would reduce background photon counts dramatically, and these can be reduced further using narrow filters at the wavelength of the QKD photons as well as spatial filtering. For example, 1-nm interference filters can be used and even narrower atomic vapor filters ($\sim 10^{-3}$ nm) are possible.

We now consider the rate at which QKD photons would be received at a satellite from a ground station transmitter. We will assume 20-cm diameter optics at both the transmitter and satellite receiver, leading to a $\sim$ 1-m diameter diffraction-limited spot size at the 300-km altitude satellite. However, there will be beam-wander owing to turbulence which can be as much as $\sim$ 10 times the diffraction limit (i.e., 10 arc-seconds of wander) so that the photon collection efficiency at the satellite is $\sim 10^{-4}$. Thus, with a laser pulse rate of 10 MHz, one photon-per-pulse on average and an atmospheric transmission of $\sim$ 80%, photons would arrive at the detector at a rate of $\sim$ 1 kHz. Then, with a 65% detector efficiency and allowing for the 25% intrinsic efficiency of the quantum cryptography protocol, a key generation rate of $\sim$ 150 Hz is feasible. With a beam tilt feedback system to keep the beam directed onto the satellite the key rate could be increased by a factor of 100. We must also consider the error rate.

We first consider errors arising from background photons arriving at the satellite. On a night time orbit with a full moon a typical radiance observed at the satellite at the transmission wavelength would be $\sim 1$ mW m$^{-2}$ str$^{-1}$ $\mu$m$^{-1}$ or $\sim 4\times10^{16}$ photons s$^{-1}$ m$^{-2}$ str$^{-1}$ $\mu$m$^{-1}$. On a night with a new moon we take the background to be $\sim 10^{15}$ photons s$^{-1}$ m$^{-2}$ str$^{-1}$ $\mu$m$^{-1}$. We will assume that the receiver "sees" a solid angle $\sim$ five times the apparent size of the source (i.e., 5 arc-seconds) and that there is a 1-nm bandwidth interference filter placed in front of the detector, giving a background photon arrival rate of $\sim$ 150 Hz (full moon); and $\sim$ 4 Hz (new moon). With a 1-ns long time window on the detector, the probability of a background photon detection would be $\sim 10^{-7}$ (full moon); and $\sim 2.5\times10^{-9}$ (new moon) per 1-ns window. The single photon detector would only be triggered for precursor bright pulses that impinge on the satellite, giving approximately 120 detector triggers per arriving QKD photon, or 800 detector triggers per detected QKD photon. The bit error rate (BER) from background photons would therefore be $\sim 10^{-4}$ (full moon); and $\sim 2\times10^{-6}$ (new moon). Assuming a detector dark count rate of 50 Hz the BER will be dominated by background photons during full moon periods, and by detector noise during a new moon, with a BER $\sim 5\times10^{-5}$.

On daytime orbits the background radiance would be very much larger, $\sim 10^{22}$ photons s$^{-1}$ m$^{-2}$ str$^{-1}$ $\mu$m$^{-1}$. Nevertheless, with an atomic vapor filter the rate of arrival of background photons would only be $\sim$ 40 kHz (assuming a $10^{-3}$ nm filter width). The BER from this background would then be $\sim$ 2%.

From this simple analysis we see that QKD between a ground station and a low-earth orbit satellite should be possible on night time orbits and 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. A cryptographically useful quantity of key material could therefore be generated for this application.

### 2.2 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

**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 |

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]."

### 2.3 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.

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

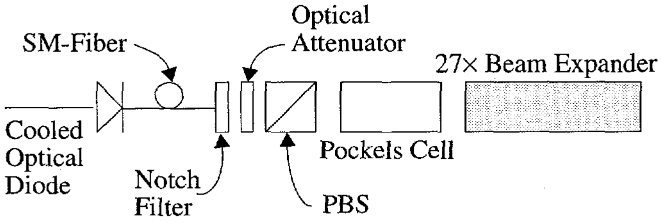

**Fig. 1.** QKD Transmitter.

computer control system (Bob). Each laser pulse is launched into free-space through the notch filter, 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 [20]. (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, $P^{\bar{n}}$, with an average photon number of $\bar{n} = 0.1$, for every 1000 pulses there will be ~ 905 empty pulses, ~ 90 pulses of 1 photon, ~ 5 pulses of 2 photons, and ~ 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.

### 2.4 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[1] followed by a PBS to test for $|r\rangle$ (again, perhaps

[1] A polarization controller was not required along the upper path because the 50/50 BS transmitted the $P$ polarization (the component of polarization parallel to the plane of incidence) without introducing any phase shift, but the quarter- and half-wave retarder pair was necessary along the lower path because the BS reflected the $P$ and $S$ (component of polarization normal to the plane of incidence) polarizations differently, introducing some ellipticity to the reflected wave.

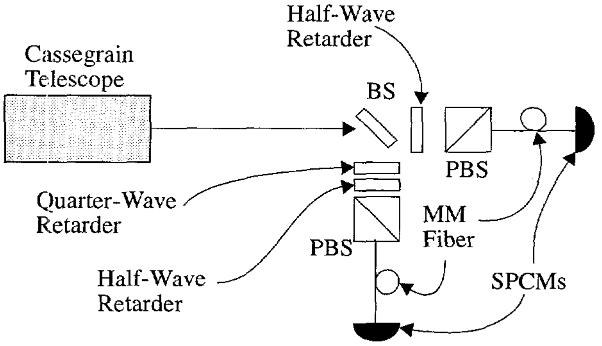

**Fig. 2.** QKD receiver.

confusing, but an $|r\rangle$ photon traveling this path is converted to $|\ell\rangle$, resulting in a 50% detection probability). 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 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 $|r\rangle$ 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), but 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 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.

### 3.1 System Efficiency

In determining Bob's bit-rate, we consider that a BS partitions a weak photon stream in a binomial fashion [20]. 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, if Alice transmits $|h\rangle$ and Bob analyzes with $|\ell\rangle$, or if Alice transmits $|r\rangle$ and Bob analyzes with $|v\rangle$. In addition, we treat the detectors as BSs with transmission coefficient $T_D = 0.65$, or in other words, that the detector, with efficiency $\eta_D = 0.65 = T_D$, also detects photon streams in a binomial way. We also treat the transmission and reception efficiency $\eta$—or power losses between the transmitter and receiver together with the losses which occur coupling power into the receiver's MM fibers—as random binomial processes. From the general form of the binomial probability distribution, we have

$$p^n_{\geq 1} = \sum_{m=1}^{n} \binom{n}{m} T^m R^{n-m} , \tag{1}$$

the probability that at least 1 photon out of $n$ photons will be transmitted through the optical elements along the optical path (this is important because the detector responds to one or more photons). The net 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.

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

where $T \mapsto \eta \cdot \eta_D/4$, $\eta$ and $\eta_D$ are as previously defined, and the factor of $1/4 = 1/2 \cdot 1/2$ gives the probability that a photon collected at the receiver, of either $|h\rangle$, or $|r\rangle$, will be transmitted through the 50/50 BS followed by the effective quarter-wave retarder and PBS (for an $|h\rangle$ photon), or the half-wave retarder and PBS (for an $|r\rangle$ photon).

These binomial expanded products (Eq. 2) of $\eta$, $1/4$, and $\eta_D$, are convolved with the Poisson probabilities, $P^{\bar{n}}_n$ that there will be exactly $n$ photons in a pulse given that the average number of photons per pulse is $\bar{n}$:

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

The convolution is then 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, $R_B$:

$$R_B = R_A \sum_{n=1}^{\infty} P^{\bar{n}}_n [1 - (1 - \eta\, \eta_D/4)^n] . \tag{4}$$

**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 | 11**0**1000000 | 1010101101 |
| A | 1111100111 | 1110111101 | 0100110100 | 1011101111 |
| B | 111110**0**011 | 1110111101 | 0100110100 | 1011101111 |

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.

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 the photon 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 $R_B = R_A/4$, which shows that Bob and Alice sacrifice 75% of their bits for privacy in agreement with Sec. 2.2.

### 3.2 Error Rate

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.

Spatial filtering reduced the ambient background ($\sim 1.1$ kHz), and the narrow gated coincidence timing windows ($\sim 5$ ns) reduced bit errors caused by the ambient background to less than $\sim 1$ every 9 s. 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. 2.2) 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.

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. More complicated error detection codes could be employed to detect these as well, such as cyclic redundancy codes [22], but this was not done in our proof of principle experiment.

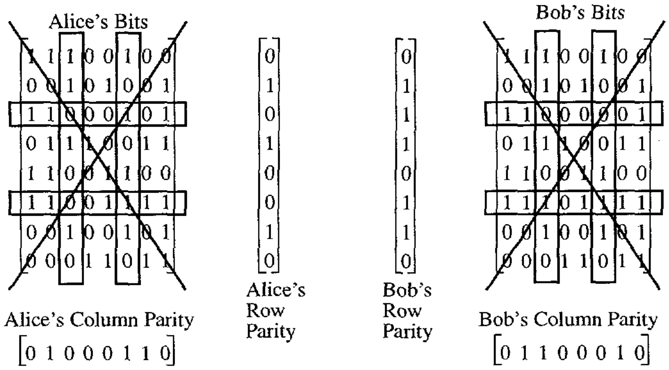

**Fig. 3.** Two-dimensional parity check scheme.

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 [21, 22], *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.[2]

To test our error detection scheme, we simulated random bit strings, with errors, and found that key material with bit errors as low as a few tenths of a percent had to be processed with the detection protocol at least twice to reduce errors to negligible levels. For random bit strings with high BERs (BERs of more than a couple of percent), small 2D matrices were needed on the first pass, but with each subsequent detection pass a larger 2D matrix could be used. We found that bit strings with BERs as high as 10% could be reduced to an estimated $\sim 1$ 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.[3] (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%.)

## 4 Eavesdropping: an Attack by Eve

Much has been said about the security of QKD against attack by an eavesdropper [19]. There are essentially two types of attack to consider: opaque attacks and translucent attacks.

### 4.1 Opaque Attack

In an opaque attack, 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%.[4] 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.

[2] We only detect and eliminate errors, and do not attempt to correct them.

[3] We used square matrices of an odd size (7 by 7 and 13 by 13) in our simulations, but decided against using them in our experiments when we determined that the elimination of the diagonals of the matrices of odd size was insufficient to ensure security.

[4] In a real system, Eve will experience reception losses associated with the collection, fiber launch and detection of the single photons.

If Eve can collect, measure, and quickly retransmit the bits she detects, she can then listen to Alice's and Bob's open bit reconciliation protocol (see Sec. 2.2). And, while Bob never reveals his bits values, Eve still knows what bits Alice and Bob commonly share because she knows when Alice began transmitted random bits. 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, i.e., Eve discards $(1 - 1/4)$, but Alice discards $(1 - 1/16)$.

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.[5] 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. However, in an imperfect experimental system dual-fire errors will occur, because 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.)

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 are each followed by an SPCM then both SPCMs will fire.

The component of a right-circular polarized pulse that 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 quantum transmission with a BS. In this scheme, Eve receives the binomial reflection probability of the BS she uses to reflect photons toward her receiving optics, and Bob receives the

[5] In B92 it is possible to send bright classical pulses of the appropriate polarization to ensure that every bit transmitted is detected at the receiver.

binomial transmission probability of the BS Eve uses. In a translucent attack it is necessary to consider Eve's and Bob's reception and detection efficiencies, which are independent; Eq. 5 shows the amount of information on the key Eve receives as a function of the reflection coefficient, $R^E = 1 - T^E$, of BS she uses in her translucent attack, her receiver efficiency $\eta_E$, and her detector efficiency, $\eta_D^E$. Equation 6 shows the amount of key Bob receives as a function of the transmission coefficient, $T^E$, of the BS Eve uses in a translucent attack, and his reception and detection efficiencies, $\eta_B$ and $eta_D^B$.

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

and

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

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 $P$, or the percentage of information Eve possesses on Alice's and Bob's common key, is determined as the ratio of the number of bits Eve and Bob share (observe coincidently) to the number of bits Alice and Bob share. First of all, if there is only 1 photon in a pulse, then either Eve or Bob will receive it, but not both. Based on this premise, Eq. 7 shows the number of bits that Bob and Eve will share if Eve attacks the key with a BS of transmission coefficient $T_E$, and reflection coefficient $R_E = 1 - T_E$.

$$N_{B \wedge E} = R_A \sum_{n=2}^{\infty} P_n^{\bar{n}} \sum_{m=1}^{n-1} \binom{n}{m} T_E^m R_E^{n-m} [1 - (1 - \frac{\eta_B \eta_D^B}{4})^m][1 - (1 - \frac{\eta_E \eta_D^E}{4})^{n-m}] \tag{7}$$

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

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

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, and if Bob's and Eve's system and detection efficiencies are equal, then for every 250 bits Eve and Bob acquire, Eve will commonly share ~ 3 of her 250 bits with Bob's 250 bits, or ~ 3/250 of Alice and Bob's common key. In fact, because Eve's knowledge on Alice's and Bob's common key is coupled to hers and Bob's system efficiencies, this situation represents the maximum amount of information Eve can obtain on Alice's and Bob's common key even if her system is perfectly efficient and Bob's is not. The inverse is also true, i.e., if Bob's system is more efficient than Eve's, then the amount of information Eve can determine on Alice's and Bob's common key decreases. (Note: at this point, we have only been able to show this empirically, but we have found no exceptions to these facts). Eve could determine which bits she commonly shares with Bob when Alice and Bob reconcile their common bits.

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 [23]" 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 [24]" encryption—also known as the Vernam Cipher: the only provably secure encryption method—and could also support any other symmetric key system.

## 5 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. 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.

## References

1. C. H. Bennett, and Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Proc. of IEEE Int. Conf. on Comp., Sys., and Sig. Proc., Bangalore, India (1984) 175.
2. A. J. Menezes, van Oorschot, P. C., and Vanstone, S. A.: *Handbook of Applied Cryptography.* CRC Press, New York (1997).
3. A. Muller, Breguet, J., and Gisin, N.: Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. Europhys. Lett. **23** (1993) 383.
4. A. Muller, Zbinden, H., and Gisin, N.: Quantum cryptography over 23 km in installed under-lake telecom fiber. Europhys. Lett. **33** (1996) 335.
5. P. D. Townsend, Rarity, J. G., and Tapster, P. R.: Enhanced single-photon fringe visibility in a 10 km-long prototype quantum cryptography channel. Elec. Lett. **29** (1993) 634.
6. C. Marand, and Townsend, P. D.: Quantum key distribution over distances as long as 30 km. Opt. Lett. **20** (1995) 1695.

7. J. D. Franson, and Ilves, H.: Quantum cryptography using optical fibers. Appl. Opt. **33** (1994) 2949.
8. R. J. Hughes, Alde, D. M., Dyer, P., Luther, G. G., Morgan, G. L., and Schauer, M.: Quantum cryptography. Contemp. Phys. **36** (1995) 149.
9. R. J. Hughes, Luther, G. G., Morgan, G. L., Peterson, C. G., and Simmons, C.: Quantum cryptography over underground optical fibers. Lecture Notes In Computer Science **1109** (1996) 329.
10. R. J. Hughes, Buttler, W. T., Kwiat, P. G., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M.: Secure communications using quantum cryptography. Proc. of SPIE **3076** (1997) 2.
11. W. T. Buttler, Hughes, R. J., Kwiat, P. G., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G., and Simmons, C. M.: Free-space quantum-key distribution. Scheduled for Phys. Rev. A **57** (1998).
12. B. C. Jacobs, and Franson, J. D.: Quantum cryptography in free space. Opt. Lett. **21** (1996) 1854.
13. J. G. Walker, Seward, S. F., Rarity, J. G., and Tapster, P. R.: Range measurement photon by photon. Quant. Opt. **1** (1989) 75.
14. S. F. Seward, Tapster, P. R., Walker, J. G., and Rarity, J. G.: Daylight demonstration of a low-light-level communication system using correlated photon pairs. Quant. Opt. **3** (1991) 201.
15. C. A. Primmerman, Murphy, D. V., Page, D. A., Zollars, B. G., and Barclay, H. T.: Compensation of atmospheric optical distortion using a synthetic beacon. Nature (London) **353** (1991) 141.
16. C. H. Bennett: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68** (1992) 3121.
17. J. F. Clauser: Experimental distinction between quantum and classical field-theoretic predictions for photoelectric effect. Phys. Rev. D **9** (1974) 853.
18. W. K. Wooters, and Zurek, W. H.: A single quantum cannot be cloned. Nature (London) **299** (1982) 802.
19. A. K. Ekert, Huttner, B., Palma, G. M., and Peres, A.: Eavesdropping on quantum cryptosystems. Phys. Rev. A **50** (1994) 1047.
20. B. E. A. Saleh, and Teich, M. C.: *Fundamentals of Photonics.* Ch. 11, Jon Wiley and Sons, Inc., New York (1991).
21. R. W. Hamming: *Coding and Information Theory.* Prentice Hall, New Jersey (1980).
22. J. Wakerly: *Error Detecting Codes, Self-Checking Circuits and Applications.* North-Holland, New York (1978).
23. C. H. Bennett, Brassard, G., Crepeau, C., and Maurer, U. M.: Generalized privacy amplification. IEEE Trans. Inf. Th. **41** 1915 (1995).
24. G. S. Vernam: Cipher printing telegraph systems for secret wire and radio telegraphic communications. Trans. Am. Inst. Electr. Eng. **XLV** (1926) 295.