LA-UR- 97-1099
CONF-970465--22

Secure communications using quantum cryptography

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

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 an emerging technology 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 single-photon states to generate shared key material over multi-kilometer optical fiber paths and over line-of-sight links. In both cases, 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. In our optical fiber experiment we have performed quantum key distribution over 24-km of underground optical fiber using single-photon interference states, demonstrating that secure, real-time key generation over "open" multi-km node-to-node optical fiber communications links is possible. We have also constructed a quantum key distribution system for free-space, line-of-sight transmissions using single-photon polarization states, which is currently undergoing laboratory testing.

Keywords: quantum cryptography, interferometry, optical communications

1. INTRODUCTION

Two of the main goals of cryptography are the encryption and authentication of messages to render them unintelligible to third parties and to certify that they have not been modified, respectively. 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 in some cryptographic algorithm. However, 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 communicate with single-photon transmissions using the emerging technology of quantum cryptography, or more accurately, quantum key distribution (QKD).[1] (A small amount of shared secret key material is required to initialize the system.)

The security of QKD is based on the inviolability of the laws of quantum mechanics. An adversary cannot "tap" the key transmissions owing to the indivisibility of quanta. At a deeper level, QKD resists interception and retransmission by an eavesdropper because in quantum mechanics, in contrast to the classical world, the result of a measurement cannot be thought of as revealing a "possessed value" of a quantum state. Furthermore, a unique aspect of quantum cryptography is that Heisenberg's uncertainty principle ensures that an eavesdropper's activities must produce an irreversible change in the quantum states ("collapse of the wavefunction") before they are retransmitted to the intended recipient. These changes will introduce an anomalously high error rate in the transmissions between the sender and intended recipient, allowing them to detect the attempted eavesdropping.

*email:

DISCLAIMER

Because it has the ultimate security assurance of a law of Nature quantum cryptography offers potentially attractive "ease of use" advantages over conventional key distribution schemes:[2] it avoids the "insider threat" because key material does not exist before the quantum transmissions take place; it avoids the cumbersome physical security aspects of conventional key distribution methods; and it provides a secure alternative to key distribution schemes based on public key cryptography, which are becoming vulnerable to algorithmic advances and improved computing techniques.[3] Thus, quantum key distribution enables "encrypted communications on demand," because it allows key generation at transmission time over an insecure optical communications link.

The origins of quantum cryptography can be traced to the work of Wiesner in the early 1970s, who proposed that if single-quantum states could be stored for long periods of time they could be used as counterfeit-proof money. Wiesner eventually published his ideas in 1983,[4] but they were of largely academic interest owing to the impracticality of isolating a quantum state from the environment for long time periods. However, Bennett and Brassard realized that instead of using single quanta for information storage they could be used for information transmission. In 1984 they published the first quantum cryptography protocol now known as "BB84".[5] A further advance in theoretical quantum cryptography took place in 1991 when Ekert proposed[6] that Einstein-Podolsky-Rosen (EPR) "entangled" two-particle states could be used to implement a quantum cryptography protocol whose security was based on Bell's inequalities. Starting in 1989, Bennett, Brassard and collaborators demonstrated that QKD was potentially practical by constructing a working prototype system for the BB84 protocol, using polarized photons.[7] Although the propagation distance was only about 30 cm, this experiment is in several ways still the most thorough demonstration of quantum cryptography.

In 1992 Bennett published a "minimal" QKD scheme ("B92") and proposed that it could be implemented using single-photon interference with photons propagating for long distances over optical fibers.[8] Since then, experimental groups in the UK,[9] Switzerland[10] and the USA[11,12] have developed optical fiber-based prototype QKD systems. The aim of these experiments has been to show the conceptual feasibility of QKD, rather than to produce the definitive system, or to address a particular cryptographic application. However, we have demonstrated the feasibility of low-error rate QKD over underground optical fibers that were installed for network applications.[12] We have performed QKD over 24 km of fiber throughout 1996 and we increased our propagation distance to 48 km in early 1997. For distances longer than about 100 km, QKD transmissions in free-space are more promising than in fibers, and are necessary for certain potential applications of QKD such as key generation between a low-earth orbit satellite and a ground station. We are developing a free-space QKD system for such applications and have recently achieved a transmission distance of 205 m.

The remainder of this paper is organized as follows. In section 2 we give a concise introduction to the theory of quantum cryptography. Then, in section 3 we describe the experimental considerations underlying our implementation of quantum cryptography in optical fibers and the performance of our system. In Section 4 we describe our free-space QKD system. Finally, in section 5 we present some conclusions.

2. QUANTUM CRYPTOGRAPHY: THEORY

To understand QKD we must first move away from the traditional key distribution metaphor of Alice sending *particular* key data to Bob. Instead, we should have in mind a more symmetrical starting point, in which Alice and Bob initially generate their own, independent random number sets, containing more numbers than they need for the key material that they will ultimately share. Next, they compare these sets of numbers to distill a shared subset, which will become the key material. It is important to appreciate that they do not need to identify *all* of their shared numbers, or even *particular* ones, because the only requirements on the key material are that the numbers should be secret and random. They can attempt to accomplish a secret distillation if Alice prepares a sequence of tokens, one kind for a "0" and a different kind for a "1", and sends a token to Bob for each bit in her set. Bob proceeds through his set bit-by-bit in synchronization with Alice, and compares Alice's token with his bit. He then replies to Alice telling her whether the token is the same as his number (but not the value of his bit). With Bob's information Alice and Bob can identify bits they have in common. They keep these bits, forming the key, and discard the others. If one of Alice's tokens fails to reach Bob this does not spoil the procedure, because it is only tokens that arrive which are used in the distillation process.

The obvious problem with this procedure is that if the tokens are classical objects they carry the bit values before they are observed by Bob, and so they could be passively monitored by Eve. However, it is possible to overcome this problem and generate a secure key by using "non-orthogonal" quantum states as the tokens. Several QKD protocols have been developed, but for simplicity we shall describe the minimal B92 QKD protocol[8] in terms of the preparation and measurement of single-photon polarization states.

Bob and Alice first agree through public discussion on their quantum comparison procedure. In the B92 QKD protocol Alice can produce photons with either of two non-orthogonal polarizations, vertical polarization ("*V*") or +45° linear polarization, say. Bob can make either of two non-orthogonal polarization measurements, each of which is orthogonal to one of Alice's, -45° linear polarization or horizontal polarization ("*H*"), say. The next step of the protocol is for Alice and Bob to generate their own independent sets of random binary numbers. They proceed through their sets bit-by-bit in synchronization, with Alice preparing a polarized photon for each of her bits according to the rules:

$$\begin{aligned} \text{"0"} &\leftrightarrow V \\ \text{"1"} &\leftrightarrow +45^\circ \end{aligned} \quad , \tag{1}$$

Alice sends each photon over a "quantum channel" to Bob. (The quantum channel is a transmission medium that isolates the quantum state from interactions with the "environment.") Next, Bob makes a polarization measurement on each photon he receives, according to the value of his bit as given by:

$$\begin{aligned} \text{"0"} &\leftrightarrow -45^\circ \\ \text{"1"} &\leftrightarrow H \end{aligned} \quad , \tag{2}$$

and records the result ("pass" = Y, "fail" = N). Note that Bob will never record a "pass" if his bit is different from Alice's (crossed polarizers), and that he records a "pass" on 50% of the bits that they have in common. In Figure 1 we show Alice's preparations and Bob's measurements for the first four bits of a QKD experiment.

Alice's numbers	1	0	1	0
Alice's polarization	+45°	V	+45°	V
Bob's polarization	-45°	-45°	H	H
Bob's numbers	0	0	1	1
Bob's results	N	N	Y	N

Figure 1. An example of B92 quantum key distribution

In this experiment we see that for the first and fourth bits Alice and Bob had different bit values, so that Bob's result is a definite "fail" in each case. However, for the second and third bits, Alice and Bob have the same bit values and the protocol is such that there is a probability of 0.5 that Bob's result is a "pass" in each case. Of course, we cannot predict in any particular experiment which one will be a "pass," but in this example the second bit was a "fail" and the third bit was a "pass."

To complete the protocol Bob sends a copy of his *results* to Alice, but not the measurement that he made on each bit. (It is at this data reconciliation stage that the initial key material is required for authentication. This key material can be replaced by a portion of the key material generated by QKD.) He may send this information over a conventional (public) channel which may be subject to eavesdropping. Now Alice and Bob retain only those bits for which Bob's result was "Y" and these bits become the shared key material. (In the example of Figure 1 the third bit becomes the first bit of the shared key.)

The QKD procedure distills one shared bit from four initial bits because it only identifies 50% of the bits that Alice and Bob actually have in common. However, this inefficiency is the price that Alice and Bob must pay for secrecy. The inventors of QKD proposed that the key bits should be used for the encryption of communications using the unbreakable "one-time pad" method.[13] However, the key material could equally well (and more practically) be used by Alice and Bob in any other symmetric key cryptosystem. For example, they could use a short

string of their key bits as an input "seed" to a cryptographically secure random number generator, whose output would provide a "key expansion" to many secure bits for use in subsequent encryption.

An eavesdropper performing her own measurement of Alice's states on the quantum channel (using Bob's measurement basis for example) will introduce a 25% error rate between Alice and Bob's key material owing to the phenomenon of wavefunction collapse. Alice and Bob can test for eavesdropping by agreeing to sacrifice a portion of their key material to test for the error rate. If this error rate is as high as 25% they will know that Eve has been monitoring their transmissions and that they should discard the whole set of key material. In practice, if the error rate is acceptably low Alice and Bob can use this information to implement a suitable error correction procedure to remove errors arising from experimental imperfections. This can then be followed by a further stage of "privacy amplification" to reduce any partial knowledge acquired by Eve to an arbitrarily low level.[14] These additional stages are performed over a public channel.

3. QUANTUM CRYPTOGRAPHY: EXPERIMENTAL REALIZATION IN OPTICAL FIBER

Although single-photon polarization states are a convenient way to describe QKD any two-state quantum system may be used for QKD. Single-photon states which are more suited to long propagation distances in optical fibers can be constructed by allowing a photon to impinge on a beamsplitter. Alice and Bob may construct this interferometric version of QKD if Alice has a source of single photons that she can inject into a Mach-Zehnder interferometer in which she controls the phase, ϕ_A, along one of the optical paths. Bob has a single-photon detector at one of the output ports and controls the phase, ϕ_B, along the other optical path.[1] (See Figure 2 in which we have indicated the sequence of optical phases corresponding to the bit sequences in the example of section 2.)

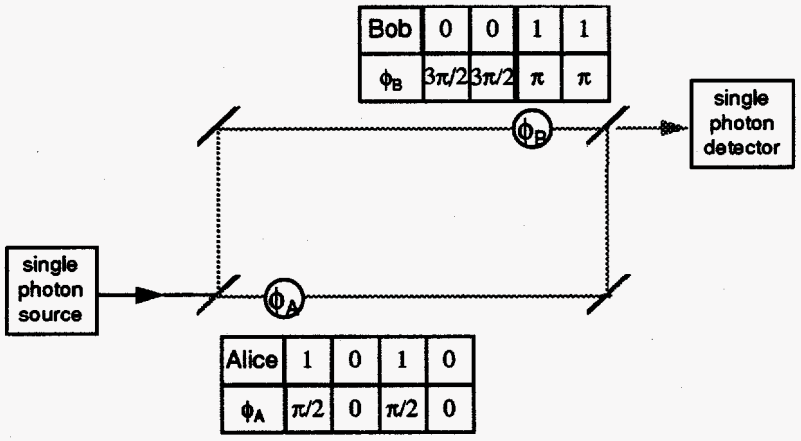

Figure 2. An interferometric realization of B92 quantum key distribution.

The probability that a photon injected by Alice is detected by Bob

$$P_D = \cos^2\left(\frac{\phi_A - \phi_B}{2}\right) , \tag{3}$$

depends on *both* paths and exhibits the phenomenon of single-photon interference between the propagation amplitudes for the upper and lower paths: the detection probability varies between 1 (equal path lengths, constructive interference) and 0 (path difference of half a wavelength, destructive interference). Of course, total probability is conserved, and the remaining probability corresponds to the photon emerging from Bob's unused exit port of the interferometer. Thus, if Alice and Bob use the phase angles $(\phi_A, \phi_B) = (0, 3\pi/2)$ for their "0" bits (respectively) and $(\phi_A, \phi_B) = (\pi/2, \pi)$ for their "1" bits they have an exact representation of B92. Each path length is analogous to one of the polarizer angles in the explanation of B92 in the previous section. (Other single-particle QKD protocols, such as BB84,[5] can be realized with different choices for the phase angles.)

To construct a practical quantum cryptography device using single-photon interference we must consider the propagation medium and detection of "single photons." Optical fibers are an obvious choice because they are widely used in telecommunications and there are commercially available components, possibly allowing a system to be constructed that can perform quantum cryptography over an installed communications system. However, although optical fibers possess the good feature of guiding photons from source to detector, their properties largely determine the operating characteristics of a system. For example: what wavelength should we choose to operate at? Two factors are relevant to this question. At what wavelengths is single-photon detection possible with non-negligible efficiency? and at what wavelengths do optical fibers have low attenuation?

For photons in the wavelength range of 600-800 nm commercially available single-photon counting modules based on silicon (Si) avalanche photodiodes (APDs) have high efficiencies and low noise rates. However, the attenuation of (single-mode) optical fibers is quite high in this wavelength range (~ 3 dB/km), which would adversely affect the data rate and the noise rate if we choose to operate in this region. Conversely, optical fibers have much lower attenuation in the infra-red at the 1.3-μm wavelength (~ 0.3 dB/km), and lower again at 1.55 μm, but although there are commercially available germanium (Ge) and indium-gallium arsenide (InGaAs) APDs that are sensitive to light at these wavelengths, there are no commercially available single-photon counting modules. Nevertheless, several groups have shown that Ge APDs can detect single photons at 1.3 μm if they are first cooled to reduce noise, and operated in so-called Geiger mode, in which they are biased above breakdown.[15] An incoming photon liberates an electron-hole pair, which with some probability initiates an avalanche current, whose detection signals the arrival of the photon. For our project we decided that the propagation distance advantages of the 1.3-μm wavelength were such that we characterized the performance of several (Fujitsu) APDs (both Ge and InGaAs) for single-photon detection at this wavelength.

Several parameters are important in characterizing the detector performance: single-photon detection efficiency; intrinsic noise rate (dark counts); and time resolution. We measured absolute detection efficiencies of 10 - 40%, (for InGaAs APDs), but noise rates that are ~ 1,000 times higher than for Si-APD photon counting modules at 800 nm. (See Figure 3 for example.) However, our detectors also have very good time resolutions, which can be utilized to compensate for the higher intrinsic noise rate because of the low dispersion of optical fibers at 1.3 μm. Thus, if a 1.3-μm photon is injected into a fiber in a short wavepacket (300-ps, say) it will emerge from the far end without being significantly delocalized and so, because we know that the photon will be expected within a short time window we need only consider the probability of a noise count in this short time interval. This probability is only ~ 5×10^{-6} at the 50-kHz noise rate for 20% efficiency in the InGaAs device shown in Figure 3.

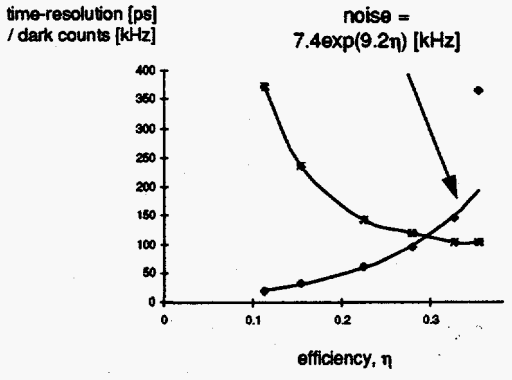

Figure 3. Geiger-mode operation of InGaAs avalanche photodiode: time-resolution and dark counts versus single-photon detection efficiency.

If we were to use different optical fibers for each of the interfering paths in the interferometric realization of B92 in Figure 2, we would have a very unstable interferometer for all but the shortest propagation distances. However, a more stable system can be produced by multiplexing both paths onto a single fiber in a design first proposed by Bennett.[8] In this design Alice and Bob have identical, unequal-arm Mach-Zehnder interferometers with a "short" path and a "long" path, with one output port of Alice's interferometer optically coupled to one of

the input ports of Bob's. The difference of the light travel times between the long and short paths, ΔT, is much larger than the coherence time of the light source, so there can be no interference within each small interferometer. However, interference can occur within the coupled system (see Figure 4).

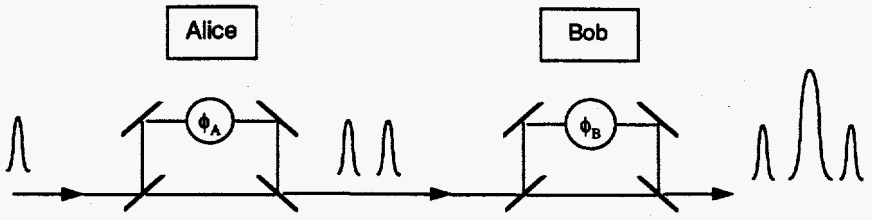

Figure 4. Time-multiplexed interferometer for quantum key distribution.

A photon injected into one of the input ports of Alice's interferometer from an attenuated pulsed laser source therefore has a 50% probability of entering Bob's interferometer, in a wave packet that is a coherent superposition of two pieces that are separated in time by ΔT, corresponding to an amplitude for it to have taken the "short" path, and a delayed component which took the "long" path. On entering Bob's interferometer each component of the wave packet is again split into a "short" component and a "long" component, so that at each output port there are three "time windows" in which the photon may arrive. The first of these ("prompt") corresponds to the "short-short" propagation amplitude; which is followed after a delay of ΔT by the "central" component comprising the "short-long" and "long-short" amplitudes; and finally, after a further time ΔT, the "delayed" time window corresponds to the "long-long" amplitude.

There is no interference in the "short-short" or "long-long" amplitudes, so the probability that the photon arrives in either of these time windows in either of Bob's output ports is 1/16 (we assume 50/50 beamsplitters and lossless mirrors). However, because the path-length differences in the two small interferometers are identical (to within the coherence length of the light source) interference does occur in the "central" time window between the "short-long" and "long-short" amplitudes. Indeed, because Alice and Bob can control the path length of their "long" paths with adjustable phases ϕ_A or ϕ_B, respectively, the probability that the photon emerges in the "central" time window at the detector in the output port shown in Figure 4 is

$$P = \frac{1}{8}\left[1 + \cos(\phi_A - \phi_B)\right] \quad . \tag{4}$$

Note that within a factor of four this expression is identical with the photon arrival probability for the simple interferometric version of B92, and that, of the two interfering paths one ("long-short") is controlled by Alice and the other ("short-long") is controlled by Bob just as in the simple interferometer of Figure 2. Thus, by sacrificing a factor of four in data rate this time-multiplexed interferometer can be used to implement QKD based on single-photon interference. (Photons arriving in the prompt and delayed time windows provide "which path" information and are useful to test for a highly invasive Eve.)

We have constructed an optical fiber version of this time-multiplexed interferometer in which each of Alice's and Bob's interferometers are built from two 50/50 fiber couplers. The output fiber legs from the first coupler convey the photons to the input legs of the second coupler via a long fiber path or a short path (ΔT~3 ns). One of the output legs of Alice's interferometer is connected by a 24-km long optical fiber path to one of the input legs of Bob's interferometer. (See Figure 5.) This 24-km path is over underground optical fibers. Photons emerge from Alice's interferometer, located in our laboratory, and are conveyed through fiber jumpers to one of the underground fibers and thence to a remote location. At this far point the photons pass through more jumpers and back onto a second fiber for the return journey back to Bob's interferometer, which for convenience is also located in our laboratory. The total travel time over the underground link is about 80 μs, with 10 dB of attenuation owing to the fiber's 0.3-dB/km attenuation and four connections along the path. This path represents a realistic test environment for quantum cryptography because of the diurnal temperature variations and other influences that

could affect the photons' propagation that are outside of our control. Finally, photons emerge from one of the output legs of Bob's interferometer into a fiber pigtailed, cooled InGaAs APD detector.

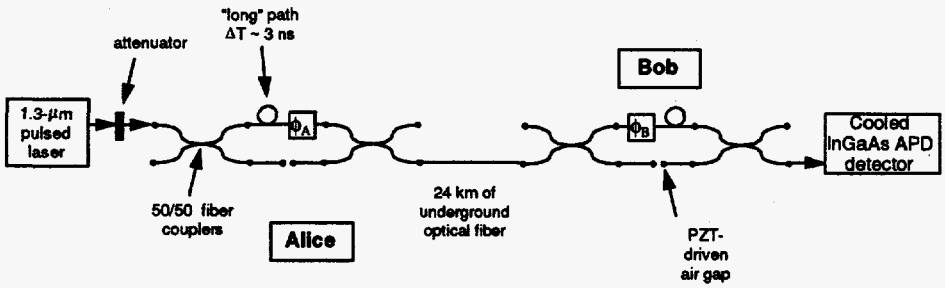

Figure 5. Schematic representation of the 14-km quantum cryptography experiment.

A "single-photon" is generated by applying a 300-ps electrical pulse with a 10-kHz repetition rate to a low-power, fiber-pigtailed semiconductor laser whose output in then attenuated before coupling into the interferometer. Each "single-photon" pulse is preceded by a bright reference pulse, introduced from an optical impulse generator attached to the lower input leg of Alice's interferometer (not shown in Figure 5), to provide arrival time information to Bob. This bright pulse triggers a room-temperature detector in the upper output leg of Bob's interferometer (not shown), which provides the "start" signal for a time-interval analyzer and triggers the pulsed-bias gate signal to the cooled single-photon detector after a delay corresponding to the single-photon emission time relative to the bright pulse emission time. Single-photon arrival is indicated by the cold detector avalanche signal which also acts as the "stop" signal for the time interval analyzer. (Although Alice and Bob are located side-by-side in our laboratory there is no direct electrical connection between the sending and receiving electronics: their only links are the 24-km optical fiber "quantum channel" and the Ethernet "public channel" connection between their two independent computer control systems.) Figure 6 is an example of photon arrival time spectra for four different phase differences that were set by driving airgaps located in the "short" paths with piezo-electric transducers (PZTs).

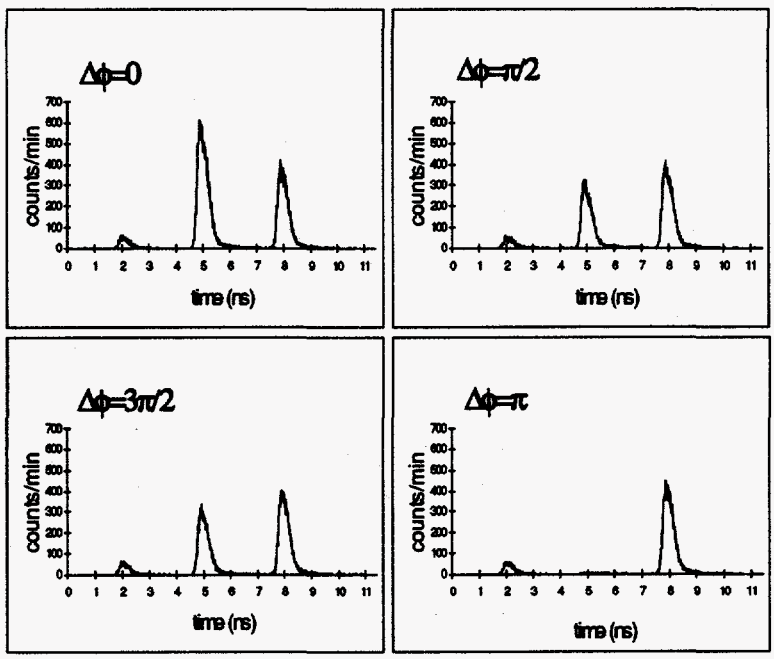

Figure 6. Photon time-of-arrival spectra accumulated at four phase difference values in the interferometer of Figure 5.

Photon counts were accumulated for 60s at each phase setting. The 3-ns separation of the different paths is clearly visible, as is the 300-ps width of the laser pulse. The unequal height of the "short-short" (leftmost in each plot) and "long-long" (rightmost) peaks is due to attenuation in the air gaps. (This asymmetry is useful for detection of a "man-in-the-middle" attack by Eve.[8]) Polarization control was necessary within the interferometers in order to achieve the high visibility single-photon interference that is apparent in the central peak. The average number of photons per laser pulse arriving in the central peak maximum was $\bar{n} = 0.4$, which is somewhat too large to provide protection against a beamsplitting attack by Eve, but adequate to illustrate single-photon interference. Some noise counts are visible in the spectra, and after accumulating time spectra at other phase settings a background subtraction was performed on the central peaks, yielding an underlying interferometric visibility of 98.4±0.6%. From the perspective of QKD this separation of the visibility is not as useful as the total probability of a count in the central time-window when the phase difference is π, because this quantity determines the error rate of the B92 protocol.

A B92 key generation procedure starts with two independent computer control systems (Alice and Bob) generating strings of random numbers by digitizing electrical noise. These random numbers are next sequentially converted into voltages that are applied to either electro-optic phase modulators (for high speed key generation) or to the PZT-driven mirrors (for low-speed key generation). A lower photon number per pulse than in Figure 6 is used to protect against a beamsplitting attack. Detected photons are recorded by Bob's computer to identify bits shared with Alice. A file containing the detected photon bit positions is then communicated to Alice over an Ethernet connection, enabling her to complete the key generation procedure. (BB84 key generation could also be implemented with a straightforward change of the computer control software.) A sample of 560 raw key bits with a 1.6% bit error rate (BER) is shown is Figure 7.

```
A  00001110  01101110  10001010  01011000  11111011  11111101  00001111
B  00001110  01101010  10001010  01001000  11111011  11111101  00001111

A  00100010  10011111  00100010  11011011  00000100  11001010  00001001
B  00100010  10011110  01100010  11011011  00000000  11001010  00001001

A  10100001  01100011  00101000  11100101  11010000  10010000  01001011
B  10100001  01100011  00101000  11100101  11010000  10010000  01001011

A  00101101  00101011  10101011  10010001  01111100  11111011  10100000
B  00101101  00101011  00101011  10010001  01111100  11111011  00100000

A  01101100  00110001  10010110  01000111  00001001  11100111  00100101
B  01111100  00110001  10010110  01000111  00001001  11100111  00100101

A  11100010  00010100  11110111  11000110  10111111  10011010  01001001
B  11100010  00010100  11110110  11000110  10111111  10011010  01001001

A  00110111  01010000  11000011  11001101  11111100  00010100  01010001
B  00110111  01010000  11000011  11001101  11111100  00010100  01010001

A  11010001  01001110  01101110  01011001  11001110  00000110  01010100
B  11010001  01001110  01101110  01011001  11001110  00000110  01010100

A  11000010  10001000  10010110  10000001  00111111  10111000  10101000
B  11000010  10001000  10010110  10000001  00111111  10111000  10101000

A  00000010  10010101  10001010  00010000  10011101  10010100  11000001
B  00000010  10010101  10001010  00010000  10011101  10010100  11000001
```

Figure 7. A 560-bit sample of Alice's (A) and Bob's (B) raw key material generated by QKD

The key material above contains errors arising from visibility imperfections and detector noise. We remove these errors by a simple block-parity check procedure to identify blocks with single error, which are then discarded. A single bit is dropped from each block that passes the parity check to compensate for the information revealed publicly. At this time we have not implemented a privacy amplification stage, but we do have a "one-time pad" encryption scheme in which we can encrypt short messages that are transmitted between the Alice and Bob computer systems over their Ethernet connection.

Several factors make the key generation rate of our QKD system considerably slower than the laser pulse rate. Firstly, the "single-photon" requirement introduces a reduction in rate because for the majority of the laser pulses no photon enters the interferometer. Then there are attenuation losses during propagation, which amount to about a factor of ten in our experiment. The QKD procedure itself has an intrinsic inefficiency of only identifying one shared bit from four initial bits. Finally, there is the detector efficiency to be included, which in our case was 20%. There is a trade-off between key-rate, which increases with detector efficiency, and BER which also increases (exponentially) with efficiency. Thus for any specific distance there will be an optimal detection efficiency giving the least BER. In our experiment this would occur for 11% detection efficiency giving a BER of 1.1%.

4. FREE-SPACE QUANTUM CRYPTOGRAPHY

In a separate project we are developing another quantum cryptography system using photon transmission in free-space, which uses non-orthogonal polarization states. This system could be used over line-of-sight terrestrial links, from the ground to an aircraft, between two aircraft, or between a ground station and a satellite in low-earth orbit. Very long distance encrypted communications between two ground stations could be accomplished with a satellite relay.

In our system a key generation procedure begins with a random number sequence being generated at the sending station. The sending station then transmits a "vertically" polarized ("V") photon for each "0" in its random number set, and a right-handed circular ("RHC") polarized photon for each "1." The photon polarization states are rapidly switched using a Pockels cell. At the receiving station each photon's polarization is randomly analyzed for "horizontal" polarization, to test for "1," or for left-handed circular (LHC) polarization, to test for "0." Thus, no photon will be detected if the receiving station's measurement is for a different bit value than the transmitted bit, but there will be a 50% detection probability if the measured and transmitted bit values are the same. Detected photons therefore allow the receiver to identify a random portion (at most one quarter) of the bits sent from the ground station. The protocol is completed by the receiving station communicating over a conventional channel the bit positions from the initial sequence for which a photon was detected (the bit value is not communicated). The sending station retains only those bits from the initial set on which the receiver detected a photon.

Single photons are generated by attenuating short pulses (~ 300ps) of light from a 772-nm temperature stabilized semiconductor diode laser. (The atmosphere has low attenuation at this wavelength.) Each single photon is preceded by a bright reference pulse for timing purposes, and to identify a short time window (~ 100 ps) in which the photon arrives. At the receiving end, cooled (- 25°C) silicon avalanche photodiode (APDs) detectors are used to detect both the bright reference pulses and the single photons with high quantum efficiency (~ 70%) and low-noise (~ 50 Hz). Coincident detection of bright pulses at each of the two receiving detectors imposes short time windows for single photon detection, and so allows a strong background rejection. A narrow interference filter, ~ 1 nm, matched with a filter in the sending optics, is used in the detection optics to reduce the background further. We have used this system to generate key material with a ~ 1% error probability at a 10-kHz sending rate over a 205-m transmission distance in our laboratory.

5. SUMMARY

We have demonstrated that low error rate quantum cryptography is feasible over long distances (24 km) of installed optical fiber in a real-world environment, subject to uncontrolled temperature and mechanical influences. This represents an important step towards the practical feasibility of quantum cryptography. However, a complete, self-contained quantum cryptography system would be able to continuously generate secret key material in unattended mode over existing optical fibers. QKD could then be incorporated into existing information security

systems so that users would be able to request an appropriate level of security for their needs and the system would deliver the corresponding quantity of key material for the particular encryption system that would be used. We are now working on the hardware and software developments requirements to achieve this goal. In our free-space experiment we plan to increase the propagation distance to several kilometers during the next six months.

ACKNOWLEDGEMENTS

It is a pleasure to thank Robert Hoffman and James Sena for their assistance in providing access to the fiber network used in these experiments. Helpful discussions with J. D. Murley, M. Kruger and M. Neergaard are gratefully acknowledged.

REFERENCES

1. For reviews see R. J. Hughes et al., "Quantum Cryptography," *Contemporary Physics* **36**, 149 (1995); C. H. Bennett et al., "Quantum Cryptography," *Scientific American* **257** no.10, 50 (1992).;
2. R. J. Hughes, "Quantum security is spookily certain," *Nature* **385**, 17 (1997).
3. D. Atkins et al., "The Magic Words are Squeamish Ossifrage," *Advances in Cryptology-ASIACRYPT '94 Proceedings*, Springer-Verlag, 1995, pp.263.
4. S. Wiesner, "Conjugate Coding," *SIGACT News* **15**, 78 (1983).
5. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore (New York, IEEE, 1984).
6. A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett.* **67**, 661 (1991).
7. C. H. Bennett and G. Brassard, "The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype is Working," *SIGACT NEWS* **20**, no. 4, 78 (1989); C. H. Bennett et al., "Experimental Quantum Cryptography," *J. Crypto.* **5**, 3 (1992).
8. C. H. Bennett, "Quantum Cryptography Using Any Two Non-Orthogonal States," *Phys. Rev. Lett.* **68**, 3121 (1992).
9. P. D. Townsend, J. G. Rarity and P. Tapster, "Single Photon Interference in 10 km Long Optical Fiber Interferometer," *Elec. Lett.* **29**, 634 (1994); P. D. Townsend, J. G. Rarity and P. Tapster, "Enhanced Single Photon Fringe Visibility in a 10-km Long Prototype Quantum Cryptography Channel," *Elec. Lett.* **29**, 1291 (1994); P. D. Townsend, "Secure Key Distribution Based on Quantum Cryptography," *Elec. Lett.* **30**, 809 (1994); C. Marand and P. D. Townsend, "Quantum Key Distribution Over Distances as Long as 30 km," *Opt Lett.* **20**, 1695 (1995).
10. A. Muller et al., "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre Over More Than 1 km," *Europhys. Lett.* **23**, 383 (1993); A. Muller, H. Zbinden and N. Gisin, "Underwater Quantum Coding," *Nature* **378**, 449 (1995); A. Muller et al., "Quantum Cryptography Over 23 km in Installed Under-lake Telecom Fibre," *Europhys. Lett.* **33**, 335 (1996).
11. J. D. Franson and H. Ilves, "Quantum Cryptography Using Optical Fibers," *Appl. Optics* **33**, 2949 (1994).
12. R. J. Hughes et al., "Quantum Cryptography Over 14 km of Installed Optical Fiber," in "Coherence and Quantum Optics VII," J. H. Eberly et al. (eds) pp.103 (Plenum, New York, 1996); R. J. Hughes et al., "Quantum Cryptography over Underground Optical Fibers," *Lecture Notes in Computer Science* **1109**, 329 (1996).
13. G. S. Vernam, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," *Trans. Am. IEE* **45**, 295 (1926).
14. C. H. Bennett et al., "Generalized Privacy Amplification," *IEEE Trans. Inf. Theory* **41**, 1915 (1995).
15. P. C. M. Owens et al., "Photon Counting Using Passively Quenched Germanium Avalanche Photodiodes," *Appl. Optics* **33**, 6895 (1994); A. Lacaita et al., "Single-Photon Detection Beyond 1μm: Performance of Commercially Available Germanium Photodiodes," *Appl. Optics* **33**, 6902 (1994).