LA-UR- 96-0624

CONF-960862--1

Title:

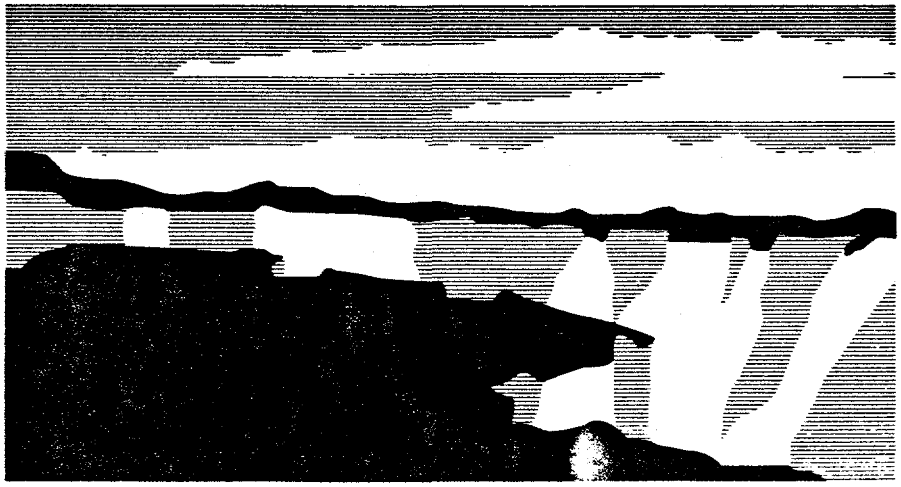
QUANTUM CRYPTOGRAPHY OVER UNDERGROUND OPTICAL FIBERS

Author(s):

Richard J. Hughes (P-23), Gabriel G. Luther (P-22), George L. Morgan (P-23), Charles G. Peterson (P-24), and Charles Simmons (P-23).

Submitted to:

CRYPTO96: Sixteenth Annual Crypto Conference
Santa Barbara, CA
August 18-22, 1996



Los Alamos
NATIONAL LABORATORY

for LA-UR

DRAFT

Quantum cryptography over underground optical fibers

R. J. Hughes,[a] G. G. Luther,[b] G. L. Morgan,[c] C. G. Peterson[d]

and

C. Simmons[e]

University of California,
Physics Division, H8C3
Los Alamos National Laboratory,
Los Alamos, NM 87545, USA

ABSTRACT

Quantum cryptography is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light whose security is based on the inviolability of the laws of quantum mechanics. An adversary can neither successfully tap the key transmissions, nor evade detection, owing to Heisenberg's uncertainty principle. In this paper we describe the theory of quantum cryptography, and the most recent results from our experimental system with which we are generating key material over 14-km of underground optical fiber. These results show that optical-fiber based quantum cryptography could allow secure, real-time key generation over "open" multi-km node-to-node optical fiber communications links between secure "islands."

a. Corresponding author: hughes@lanl.gov
b. luther@physics.lanl.gov
c. glmorgan@lanl.gov
d. peterson@lanl.gov
e. csimmons@lanl.gov

DRAFT

Quantum cryptography over underground optical fibers

ABSTRACT

Quantum cryptography is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light whose security is based on the inviolability of the laws of quantum mechanics. An adversary can neither successfully tap the key transmissions, nor evade detection, owing to Heisenberg's uncertainty principle. In this paper we describe the theory of quantum cryptography, and the most recent results from our experimental system with which we are generating key material over 14-km of underground optical fiber. These results show that optical-fiber based quantum cryptography could allow secure, real-time key generation over "open" multi-km node-to-node optical fiber communications links between secure "islands."

1. Introduction

Two of the main goals of cryptography (encryption and authentication of messages) can be accomplished, with provable security, if the sender ("Alice") and recipient ("Bob") possess a secret random bit sequence known as "key" material. The initial step of key distribution, in which the two parties acquire the key material, must be accomplished with a high level of confidence that a third party ("Eve") cannot acquire 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.

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: 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. Thus, quantum key distribution (QKD) enables "encrypted communications on demand," because it allows key generation at transmission time over an unsecure optical communications link.

The origins of quantum cryptography can be traced to the work of Wiesner, 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,[2] 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".[3] A further advance in theoretical quantum cryptography took place in 1991 when Ekert proposed[4] 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. Also in 1991, Bennett and collaborators demonstrated that QKD was potentially practical by constructing a working prototype system for the BB84 protocol, using polarized photons.[5]

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.[6] Since then, experimental groups in the UK,[7] Switzerland[8] and the USA[9, 10] 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. We have been generating key material over 14 km of fiber throughout 1995 and we anticipate increasing the propagation distance to 24 km and possibly to 31 km during early 1996.

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. Finally, in section 4 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 a minimal QKD protocol[6] (known as B92) in terms of the preparation and measurement of single-photon polarization states.

Consider a photon propagating along the x-axis. We introduce an orthonormal basis of single-photon polarization states $\{|V\rangle, |H\rangle\}$ corresponding to "vertical" (along the z-axis) or "horizontal" (along the y-axis) linear polarization, respectively. These states satisfy the orthonormality relations

$$\begin{gathered} \langle V|V\rangle = \langle H|H\rangle = 1 \\ \langle V|H\rangle = 0 \end{gathered} \quad , \tag{1}$$

and they span a two-dimensional Hilbert space. Using linear combinations of the states with complex coefficients we can construct any other single-photon polarization state. For example, the states $|+45°\rangle = 2^{-1/2}(|V\rangle + |H\rangle)$ and $|-45°\rangle = 2^{-1/2}(|V\rangle - |H\rangle)$ correspond to photon linear polarizations orientated at plus and minus 45° to the vertical axis (in the y-z plane). $\{|+45°\rangle, |45°\rangle\}$ constitutes another orthonormal basis of this Hilbert space but note that the new basis vectors are non-orthogonal to the old ones.

A (von Neumann) measurement in quantum theory is a projection operator in Hilbert space. For example, a measurement for horizontal polarization is represented by the projection operator

$$P_{|H\rangle} = |H\rangle\langle H| \quad , \tag{2}$$

and similarly a measurement for -45° polarization is represented by

$$P_{|-45°\rangle} = |-45°\rangle\langle -45°| \quad . \tag{3}$$

A photon may have a definite value with respect to a particular measurement if it is in an eigenstate of the corresponding projection operator. For example the state $|H\rangle$ is an eigenstate of the operator $P_{|H\rangle}$ with eigenvalue = 1, but note that the above two measurements do not commute:

$$\left[P_{|H\rangle}, P_{|-45°\rangle}\right] \neq 0 \quad , \tag{4}$$

which means that a photon cannot exist in a simultaneous eigenstate of both horizontal and -45° polarizations. This property of non-orthogonal states prevents an eavesdropper from acquiring complete knowledge of the key material in QKD.

The result of a measurement P on a state $|\psi\rangle$ is given by the "collapse of the wavefunction"

$$|\psi\rangle \rightarrow \begin{cases} \dfrac{P|\psi\rangle}{\| P|\psi\rangle \|} & \text{with probability } \langle\psi|P|\psi\rangle \\[2ex] \dfrac{(1-P)|\psi\rangle}{\| (1-P)|\psi\rangle \|} & \text{with probability } \langle\psi|(1-P)|\psi\rangle \end{cases} \quad , \tag{5}$$

where we shall describe the first outcome as a "pass" and the second as "fail." Here the norm is defined as

$$\| |\phi\rangle \| \equiv |\langle\phi|\phi\rangle|^{1/2} \quad . \tag{6}$$

Note that if $|\psi\rangle$ is an eigenstate of the projection P it is unaltered by the act of measurement, whereas if $|\psi\rangle$ and P are "non-orthogonal" (e.g. $|\psi\rangle = |+45°\rangle$ and $P = P_{|H\rangle}$) then the act of measurement irreversibly alters the quantum state. (In this example the state emerges as $|V\rangle$ or $|H\rangle$ with 50% probability each. Quantum mechanics cannot predict the result of any particular such measurement but instead gives the probabilities of the different outcomes that would be observed in multiple repetitions of the experiment.) It is this alteration of the quantum state by measurement that allows eavesdropping on QKD to be detected.

For the B92 protocol Alice has two non-orthogonal state preparations: $|V\rangle$ or $|+45°\rangle$; and Bob can make non-orthogonal projections onto $|-45°\rangle$ or $|H\rangle$. In the first step of the B92 protocol Alice and Bob generate their own independent sets of random binary numbers. In the second step they proceed through their sets bit-by-bit in synchronization, with Alice preparing a state for each of her bits according to the rules:

$$\begin{array}{c} "0" \leftrightarrow |V\rangle \\ "1" \leftrightarrow |+45°\rangle \end{array} \quad . \qquad (7)$$

Alice sends each state 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 measurement of each state he receives, according to the value of his bit as given by:

$$\begin{array}{c} "0" \leftrightarrow P_{|-45°\rangle} \\ "1" \leftrightarrow P_{|H\rangle} \end{array} \quad , \qquad (8)$$

and records the result ("pass" = Y, "fail" = N). Note that Bob will never record a "pass" if his bit is different from Alice's, and that he records a "pass" on 50% of the bits that they have in common. In the example in Figure 1

Alice's numbers	1	0	1	0
Alice's states	|+45°>	|V>	|+45°>	|V>
Bob's states	<-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

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

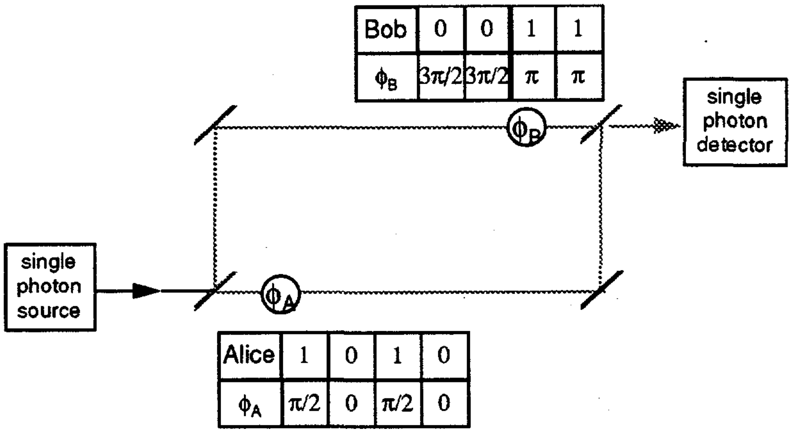
QKD.) He may send this information over a conventional (public) channel which may be subject to eavesdropping. Now Alice and Bob retain only those bits for which Bob's result was "Y" and these bits become the shared key material. (In the example of Figure 1 the third bit becomes the first bit of the shared key.) This 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.

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 described earlier. 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.

Traditionally it has been proposed that the key bits generated by QKD should be used for the encryption of communications using the unbreakable "one-time pad" method. 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.

3. Quantum cryptography: experimental realization

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. (In this context the optical phase is an angular expression of the length of the optical path: a phase change of 2π corresponds to a change in path length of one optical wavelength.) 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.)



Bob	0	0	1	1
ϕ_B	$3\pi/2$	$3\pi/2$	π	π

Alice	1	0	1	0
ϕ_A	$\pi/2$	0	$\pi/2$	0

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

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

$$P_D = \cos^2\left(\frac{\phi_A - \phi_B}{2}\right) \quad . \tag{9}$$

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. (Other single-particle QKD protocols, such as BB84,[3] 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 there are commercially available single-photon counting modules based on silicon (Si) avalanche photodiodes (APDs), which 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 will adversely affect the data rate and the noise rate if we choose to operate in this region. (The loss mechanism is predominantly Rayleigh scattering out of the fiber.) Conversely, optical fibers have much lower attenuation at 1.3 µm (~ 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 infrared 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.[11] 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 for 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.

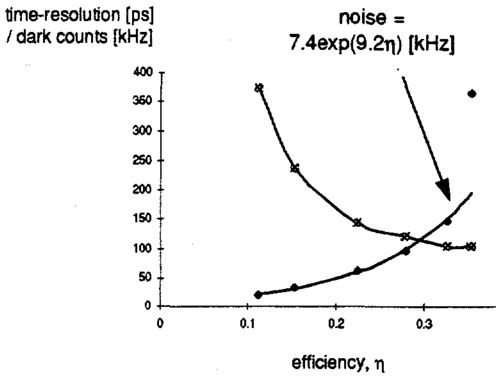


Figure 3. Geiger-mode operation of InGaAs avalanche photodiode: time-resolution and dark counts versus single-photon detection efficiency.

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.[6] 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).

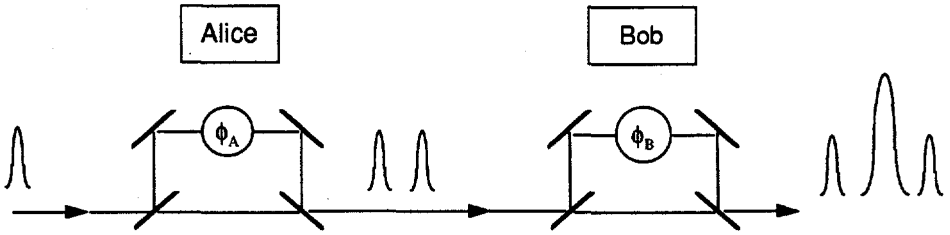


Figure 4. Time-multiplexed interferometer for quantum key distribution.

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

$$P = \frac{1}{8}\left[1 + \cos(\phi_A - \phi_B)\right] \quad . \tag{10}$$

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. (The photons "lost" in the prompt and delayed time windows 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 instead of beamsplitters. Each coupler has two input legs and two output legs: a photon entering on one leg has a 50% probability to emerge from either of the output legs. No mirrors are required because 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~5 ns). One of the output legs of Alice's interferometer is connected by a 14-km long optical fiber path to one of the input legs of Bob's interferometer. (See Figure 5.) This 14-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 67 μs, with 12.2 dB of attenuation owing to the 16 fiber 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.

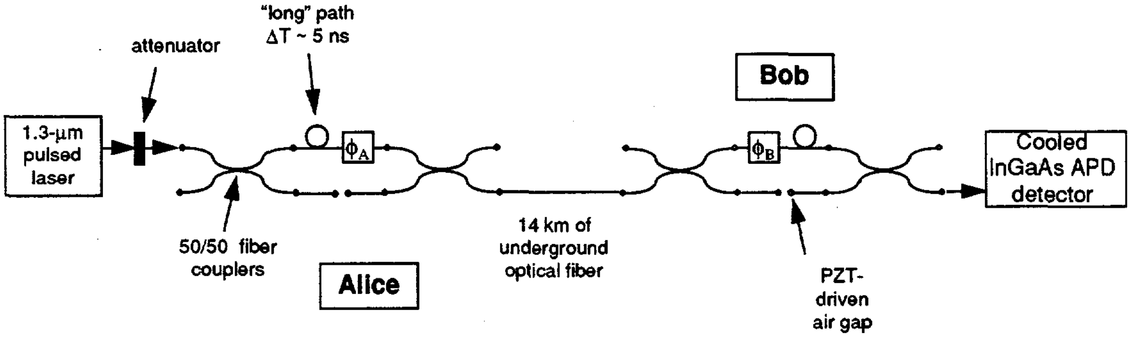


Figure 5. Schematic representation of the 14-km quantum cryptography experiment.

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. The electrical pulse is also the "start" signal for a time-interval analyzer and applies the pulsed-bias gate signal to the detector after a delay corresponding to the light transit time through the system. The detector avalanche acts as the "stop" signal. Figure 6 shows time-spectra of photon arrival times for four different phase differences that were set by driving airgaps located in the "short" paths with piezo-electric transducers (PZTs).

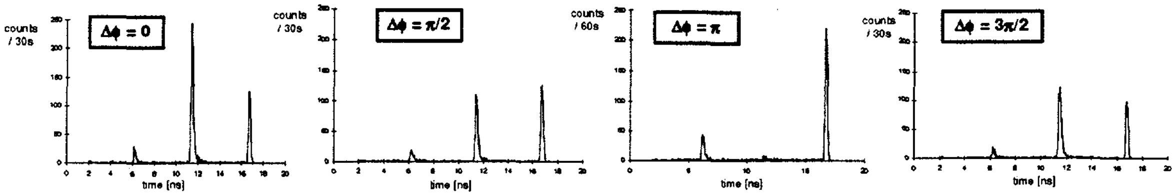


Figure 6. Photon time-of-arrival spectra accumulated at four phase difference values in the interferometer of Figure 5.

Photon counts were accumulated for 30s at each phase setting, with the exception of the π-phase shift case, in which a 60-s integration time was used, so as to collect more counts in the central peak. The 5-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.[6]) 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 $\bar{n} = 0.04$, providing protection against a beamsplitting attack by Eve even if she was located immediately after Alice's interferometer. 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 visibility of 99.6±2.8%.

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. (The probability that Bob detects a photon even though his bit value is different from Alice's determines the error rate.) Thus, the central peak in the second plot of Figure 6 represents 1264 received "1-1"s generated from $3\text{x}10^5$ initial "1-1"s (a sequence of photons for which Alice and Bob both have the "1" bit value). The central peak of the fourth plot represents 1350 received "0-0"s generated from $3\text{x}10^5$ initial "0-0"s; and the central peak of the third plot represents only 32 "0-1" errors generated from $6\text{x}10^5$ initial "0-1"s. These results give an inferred efficiency of key bit generation of $2.2\text{x}10^{-3}$ per initial random bit, and a bit error rate (BER) of 1.2%.

A key generation procedure starts with two independent computer control systems (Alice and Bob) generating strings of pseudo-random numbers which are 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). (We use pseudo-random number generation for experimental convenience. A real QKD system would require true random number generation, which could be accomplished by utilizing detector noise for instance.) 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. A sample of key material is shown is Figure 7.

```
A     01010011     01001000     01000100     10100010     10000101
B     01010001     01001000     00000100     10100010     10000101

A     01101011     10101000     11100101     00000111     01110100
B     01101011     10101000     11100101     00000011     01110100

A     10011101     00011110     01011001     10000101     01110000
B     10011101     00011110     01011001     10000101     01110000

A     01111000     11101010     11100000     00010101     11100011
B     01111000     11101010     11100000     00010101     11100011

A     10011111     01100000     11000000     00100011     10000110
B     10011101     01100000     11000000     00100011     10010110

A     00010101     00000100     10010100     10000010     10100110
B     00010101     00000000     10010100     10000010     10100110

A     00000010     01100001     01101100     11000010     11100001
B     00000010     01100001     01100100     11000010     11100001

A     11001110     01110010     10010100     01001010     01000100
B     11001110     01110010     10010100     01001010     11000100

A     10001110     11111111     01001011     00010011     11000110
B     10001110     11111111     01001011     00010011     11000110

A     10101100     10110101     10110000     01111000     01001101
B     10101100     10110101     10110000     01111000     01001101
```

Figure 7. A 400-bit sample of Alice's (A) and Bob's (B) key material generated by QKD

The key material above contains errors arising from visibility imperfections and detector noise. At present we remove these errors by a simple block-parity check procedure. At this time we have not implemented a privacy amplification stage, but we do have a simple XOR 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 the majority of the laser pulses contain no photon. Then there are attenuation losses during propagation, which amount to about a factor of fifteen in our experiment. The QKD procedure itself has an intrinsic inefficiency of only identifying one shared bit from four initial bits, which is reduced by a further factor of four in our scheme, resulting in an additional factor of sixteen reduction in key rate. 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 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. Summary

We have demonstrated that low error rate quantum cryptography is feasible over long distances (14km) of installed optical fiber in a real-world environment, subject to uncontrolled temperature and mechanical influences. This represents an important new 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.

References

1. For a review see R. J. Hughes et al., Contemporary Physics **36**, 149 (1995).
2. S. Wiesner, *SIGACT News* **15**, 78 (1983).
3. C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore (New York, IEEE, 1984).
4. A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
5. C. H. Bennett et al., *J. Crypto.* **5**, 3 (1992).
6. C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
7. P. D. Townsend, J. G. Rarity and P. Tapster, *Elec. Lett.* **29**, 634 (1994); P. D. Townsend, J. G. Rarity and P. Tapster, *Elec. Lett.* **29**, 1291 (1994); P. D. Townsend, *Elec. Lett.* **30**, 809 (1994).
8. A. Muller et al., *Europhys. Lett.* **23**, 383 (1993).
9. J. D. Franson and H. Ilves, *Appl. Optics* **33**, 2949 (1994).
10. R. J. Hughes et al., Los Alamos report LA-UR-95-2836, invited paper to appear in Proceedings of "Seventh Rochester Conference on Coherence and Quantum Optics," Rochester, NY, June 1995.
11. P. C. M. Owens et al., *Appl. Optics* **33**, 6895 (1994); A. Lacaita et al., *Appl. Optics* **33**, 6902 (1994).

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.