PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Secure Optical Communications Systems Using Quantum Cryptography

Paul D. Townsend, C. Marand, S. J. D. Phoenix, K. J. Blow and S. M. Barnett

Phil. Trans. R. Soc. Lond. A 1996 **354**, 805-817
doi: 10.1098/rsta.1996.0033

Secure optical communications systems using quantum cryptography

By Paul D. Townsend[1], C. Marand[1], S. J. D. Phoenix[1], K. J. Blow[1] and S. M. Barnett[2]

[1]*BT Laboratories, Martlesham Heath, Ipswich IP5 7RE, UK*
[2]*Department of Physics and Applied Physics, University of Strathclyde, Glasgow G4 0NG, UK*

Quantum cryptography is the result of a synthesis of ideas from fundamental quantum physics and classical encryption that may radically change the way in which the confidentiality of information and the integrity of communications networks are protected. In this paper we discuss the issues that influence the design of practical quantum cryptography schemes for optical fibre-based communication systems.

1. Introduction

Quantum cryptography (Bennett *et al.* 1983, 1992*a*, *b*), or quantum key distribution as it is more correctly described, is a technique that exploits the fundamental principles of quantum measurement, as embodied in the Heisenberg uncertainty principle, to enable the users of communication channels to exchange messages with guaranteed security. The scheme allows the users, whom we shall call Alice and Bob, to establish a shared random sequence of bits and then to verify whether or not the sequence has been monitored by an eavesdropper, Eve. If Alice and Bob confirm that the bit sequence is indeed secret then they can use it as an encryption key, and thereby exchange messages securely over any communication channel that they choose. The essential quantum property on which this scheme is based is the existence of pairs of conjugate observables such as the linear and circular polarization states of single photons, for example, that are incompatible in the sense that a measurement of one necessarily randomizes the value of other. Alice and Bob exploit this property by using such quantum states to transmit their key, and adopt a communication protocol which ensures that any eavesdropper who attempts to intercept and resend the sequence will inevitably corrupt the data. Consequently, by monitoring the error rate for their quantum transmission, Alice and Bob have a fundamental measure of the amount of information leaked to Eve, and hence can calculate whether their key is safe to use. Evidently, there is no analogue of this technique in the classical domain, since classical information is unchanged by the act of measurement. The full details of the quantum cryptography protocol are described by Barnett & Phoenix (this volume).

Quantum cryptography was developed by Charles Bennett, Gilles Brassard, Stephen Wiesner, and co-workers in the 1980s (Bennett *et al.* 1983). Their work culminated in the first proof-of-principle quantum key exchange which took place over about 30 cm of free-space in 1989 (Bennett *et al.* 1992*a*). Since then there has

Phil. Trans. R. Soc. Lond. A (1996) **354**, 805–817
Printed in Great Britain

been a great deal of interest in developing the technique in order to investigate its potential for applications in real communication systems (Townsend *et al.* 1993*a*, *b*; Muller *et al.* 1993; Franson & Ilves 1994; Franson & Jacobs 1995). We have recently moved somewhat closer to this goal at BT Laboratories with the demonstration of prototype systems up to 30 km in length (Townsend 1994*a*, Marand & Townsend 1995), and the design of quantum cryptography schemes for multiuser operation on fibre-distributed networks (Townsend *et al.* 1994*b*; Phoenix *et al.* 1995). In this paper we shall review this work and describe the important considerations that have determined the direction of the research.

2. Design criteria for practical systems

The most basic requirement for the implementation of a quantum cryptography scheme is the ability to generate, modulate, transmit and detect single quanta. As we shall see, this is currently achievable in the visible to near infrared region of the electro-magnetic spectrum, where silica-glass fibre is available as an excellent low-loss transmission medium. Perhaps the two most important factors influencing the design of a quantum cryptography system are the properties of the fibre itself, and the performance of the single-photon detectors. We illustrate these considerations in §§ 3 and 4 by reference to two experimental systems that we have recently developed. The first system has been used to demonstrate secure cryptographic-key transmission over up to 30 km of standard communications fibre at an operating wavelength of 1.3 μm (Townsend 1994*a*; Marand & Townsend 1995). At this wavelength, the loss in standard telecommunications fibre is very low ($\sim 0.35\ \mathrm{dB\ km^{-1}}$), the group velocity dispersion (GVD) is close to zero, and the fibre supports a single spatial mode. These are all favourable properties for achieving key transmission over very long distances. The detectors used in this system are conventional germanium avalanche photodiodes (APDs) which are cooled to 77 K and biased above reverse breakdown to achieve single-photon sensitivity. Although these APDs work, their operational characteristics are as yet far from optimum for quantum cryptography. Consequently, a further prototype system has also been developed which uses silicon APDs. These devices are an attractive alternative to germanium APDs, at least for near-term applications, since they are currently at a more advanced stage of development. For example, silicon APDs can be thermo-electrically cooled and have quantum efficiency values more than twice as large as germanium devices, and dark-count rates which are some 2–3 orders of magnitude smaller. These latter two parameters are important for quantum cryptography systems, since the error rate caused by a non-zero dark-count to photo-count ratio affects the ability to detect an eavesdropper. However, quantum cryptography systems using silicon APDs must operate at wavelengths shorter than 1.1 μm (the band-gap of silicon) where the fibre parameters are non-ideal. For example, the prototype system described below operates at a wavelength of 0.83 μm, where standard fibre supports two spatial modes and has relatively high values of loss $\sim 2\ \mathrm{dB\ km^{-1}}$ and GVD $\sim -90\ \mathrm{ps\ nm^{-1}\ km^{-1}}$. These factors tend to favour shorter span applications, perhaps in secure local-area networks (LANs). We discuss the use of quantum cryptography on multiuser optical networks (Townsend *et al.* 1994*b*; Phoenix *et al.* 1995) in § 4. This extension from the original point-to-point application is very important for quantum cryptography since high-capacity optical networks are likely to become of increasing technological importance in the future.

Although the fundamental principles of quantum cryptography schemes are often

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

described with reference to single-photon states, or correlated twin-photon states (Ekert 1991; Ekert *et al.* 1992), all practical demonstrations to date have in fact employed coherent or incoherent states of low average photon number. This is largely because such states are relatively easy to generate using optical attenuators and conventional lasers or light-emitting diodes, and these components are commercially available for all the wavelength ranges of interest for optical fibres. Weak coherent or incoherent sources produce superpositions or statistical mixtures of N-photon states, respectively, and their number fluctuations are described by Poisson statistics, i.e.

$$P_N = \frac{\bar{n}^N \varepsilon^{-\bar{n}}}{N!}, \tag{2.1}$$

where P_N is the probability of obtaining N photons when the average photon number is $\bar{n}$. When $\bar{n}$ is small, the contribution of the $N = 1$ state to superposition or mixture dominates that of the $N \geqslant 2$ multiphoton states, e.g. for $\bar{n} = 0.1$, $P_{N=1} \approx 0.1$ and $P_{N\geqslant 2} \approx 5 \times 10^{-3}$. Hence, pulses from such a low-intensity Poissonian source are unlikely to split at an optical coupler or beamsplitter. This is very important in the context of quantum cryptography, since it means that an eavesdropper can only obtain a limited amount of information via undetected 'beamsplitter attacks' (Bennett *et al.* 1992*a*). The penalty for this is that when $\bar{n} = 0.1$, $P_{N=0} \approx 0.9$ and therefore even if Bob has perfect detectors and the communication channel is lossless Bob will only receive one in ten of Alice's pulses. However, in practical terms this reduction in bit-rate is a worthwhile price to pay when compared to the cost and complexity of a true single-photon source.

A further design issue for a practical system arises from the choice of modulation scheme. Polarization modulation schemes have been discussed in some detail by Barnett & Phoenix (this volume) and in the following section we shall discuss an interferometric scheme that uses a phase-shift encoding technique. Perhaps the most important factor influencing the choice of modulation scheme is the commercial availability of the modulators themselves. These must be compact, low-loss, have low drive-voltage requirements and be available for operation at the wavelengths of interest for telecommunications. Currently, the devices that best fulfil these requirements are phase-modulators based on lithium niobate technology. This has led us to concentrate mainly on interferometric key distribution schemes, although a prototype polarization-encoded scheme is also discussed in § 4. Under specific operating conditions, where detector noise and polarization mode dispersion (Breguet *et al.* 1994) in the fibre are not limiting factors, polarization schemes (Muller *et al.* 1993; Franson & Ilves 1994; Franson & Jacobs 1995) exhibit superior error-rate performance compared to interferometric schemes (Marand & Townsend 1995). This is due to the fact that, in general, it is always possible to obtain polarizer extinction ratios that are larger than the fringe contrast ratio in an interferometer. Any real quantum cryptography system must be capable of recovering from the non-zero error rates that arise from these types of component deficiencies, or alternatively from low-levels of eavesdropping on the system. Secure error-correction and privacy amplification techniques have been developed to perform this task (Bennett *et al.* 1992*a*; Robert *et al.* 1988). It might be thought that the achievement of very low bit-error rates, i.e. $\ll 1\%$, in polarization-encoded quantum cryptography systems would lead to substantial reductions in the complexity of these stages of the protocol. However, since error correction and privacy amplification can be performed using high data-rate classical communication channels and fast computers, this is unlikely to be the case.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Instead, the rate-limiting step in a quantum cryptography system is always likely to be the initialization of the quantum channel and the quantum transmission itself, which has an intrinsically low bit-rate due to the dead-time associated with single-photon detectors. In a polarization-dependent modulation scheme, for example, the channel initialization involves a periodic compensation for thermally induced changes in fibre birefringence, which cause the polarization states of photons exiting the fibre to evolve with time. Hence, automated polarization-control techniques similar to those developed for coherent communications systems (Walker & Walker 1990) are required. There is thus an intrinsic trade-off between error rate and bit rate; to maintain a high polarization extinction ratio the channel must be recalibrated more frequently and to a higher level of accuracy. Consequently, our approach at BT has been to concentrate on the practicality of our systems while aiming for error rates sufficiently low (typically a few percent) to allow the application of error-correction and privacy amplification techniques.

3. Long-span point-to-point quantum key distribution

(a) *Interferometer system*

In the long-distance quantum cryptography demonstrator built at BT Laboratories we use low-intensity coherent pulses and an interferometric coding scheme (Bennett 1992; Townsend *et al.* 1993*a*) to send keys securely over up to 30 km of optical fibre. The experimental system shown in figure 1 is based on a Mach–Zehnder device (Townsend *et al.* 1993*b*), in which the source is a 1.3 μm-wavelength semiconductor laser that generates 80 ps duration pulses at a repetition rate of 1 MHz. The laser output is strongly attenuated such that the average photon number $\bar{n}$ of the pulse pairs entering the transmission fibre is about 0.1. The system is formally equivalent to a simple Mach–Zehnder interferometer with a lithium niobate phase modulator in each spatially separated arm. However, by using time and polarization division to separate the individual 'paths' in a single long transmission fibre, the device can be many km in length and yet still remain stable against environmental perturbations. Figure 1 illustrates how this is achieved by indicating the relative spatial, temporal and polarization changes experienced by the optical pulses propagating through the device. For $\bar{n} \ll 1$, these pulses can be viewed as temporal peaks in the probability amplitude distribution for the low-intensity quantum field. Pulses exiting the interferometer are detected using a time-correlated photon-counting set-up (Townsend *et al.* 1993*a*), which is based upon a liquid-nitrogen-cooled germanium APD (Lacaita *et al.* 1993; Owens *et al.* 1994). The device is operated in Geiger-mode, with the above-breakdown bias gated on for ~ 100 ns synchronously with the laser source. Coupling between the interferometer and the APD is provided by a low-loss polarization multiplexer, and pulses arriving from the '1' and '0' output ports are distinguished temporally by means of a fibre delay loop.

A basic test of the suitability of this apparatus for quantum key distribution can be obtained from a measurement of the single-photon interference fringes. Figure 2 shows the variation of the '0' and '1' count rates as the relative path length difference in a 10.8 km-long device is slowly scanned. The fringes show a high visibility value $V = 0.98$, which demonstrates that low-error-rate key transmission should be possible. The residual count rates at the fringe minima arise from detector dark counts and the intrinsic fringe visibility $V = 0.99$, which is measured at higher $\bar{n}$ values. The stability of the device is also important since any large drifts in the relative

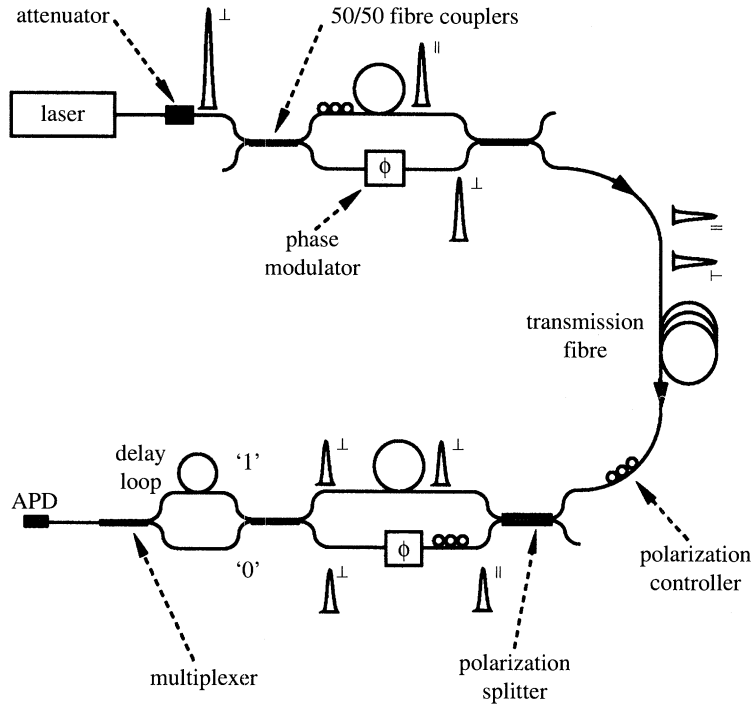

Figure 1. Interferometric quantum cryptography scheme.

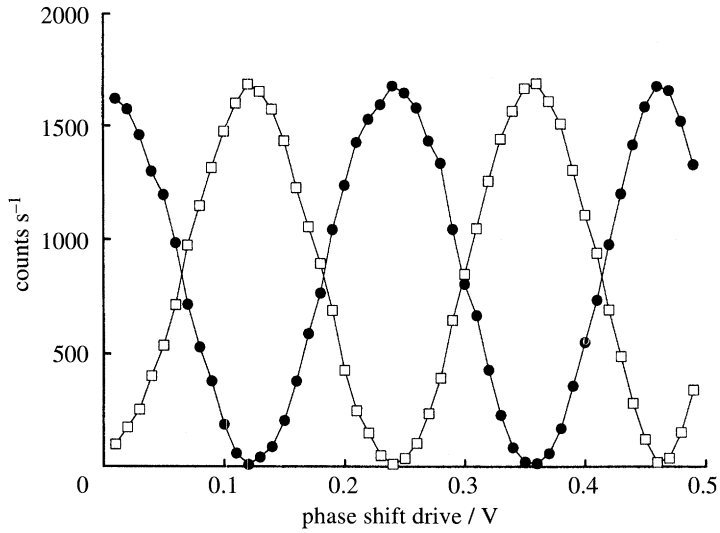

Figure 2. Interference fringes measured at the single-photon level (open squares denote the '0' count rate, filled circles the '1' count rate). The results were obtained using a 10.8 km-long interferometer and show a high fringe visibility of 0.98.

path length during key transmission will increase the error rate. In fact we find that slow thermal drift in the interferometer produces a π phase shift in 4–5 min, so key transmission is performed in bursts that are short compared with this drift time, and the interferometer is initialized in between each burst.

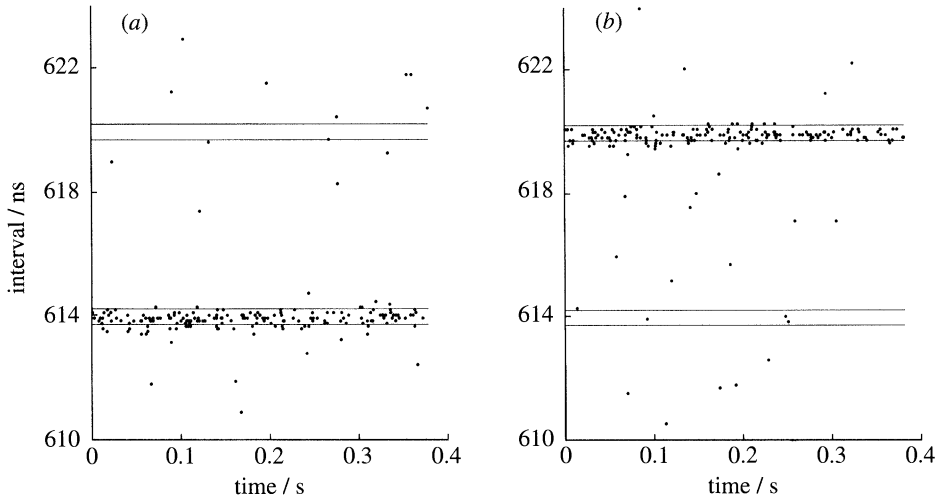

Figure 3. Key transmission results. (*a*) The fraction (approximately half) of Bob's data that was received in time slots where Alice sent a zero. Most photocounts occur within the lower '0' window, as required for a low error-rate transmission. (*b*) The fraction of Bob's data that was received in time slots where Alice sent a one. Most photocounts occur within the upper '1' window, as required.

(*b*) *Key distribution*

During key distribution, Alice randomly encodes each laser pulse with one of four possible phase shifts ϕ_A, namely $-45°$, $+135°$ (basis X) and $+45°$, $-135°$ (basis Y), where the phase-shift pair in each of the two conjugate bases represents the binary digits 0 and 1, respectively. Bob simultaneously drives his own modulator in order to randomly and independently select between measurement phase shifts ϕ_B of $-45°$ (basis X) and $+45°$ (basis Y). If a pulse is detected in a given bit period he labels it '0' or '1' according to the output port at which it was registered, and records the bit period in the data sequence when it occurred. After an appropriate time, typically after a few thousand bits have been transferred, Alice and Bob cease transmission and analyse their key data by communicating via a public channel. The first stage of this process involves Bob revealing to Alice the bit periods in which he detected a pulse and the basis that he used for each measurement (but not the result, i.e. whether he received a zero or a one). Alice then tells Bob the bit periods in which they used the same bases, and hence expect a deterministic outcome since $(\phi_A - \phi_B = 0°$ or $\pm 180°$. They then discard the other half of the data which should show no correlation, since in these cases $(\phi_a - \phi_B) = \pm 90°$ and the outcome of the interference is probabilistic, i.e. Bob is equally likely to detect the pulse at the '0' or '1' ports.

Figures 3*a* and *b* show the results of a single 400 ms-long key transmission, where each point represents a single photodetection or dark count. The *y*-axis represents the time interval between a detection event and the next laser drive pulse that follows in time. Since the optical fibre paths from the two interferometer outputs to the APD are of unequal length, the '0' and '1' photons generate time interval values that lie in two separate bands centred on 614 and 620 ns, respectively. The 0.5 ns width of each band is determined by detector timing jitter (Owens *et al.* 1995), and the points in between the bands are dark counts which occur randomly in time. The data for which Alice and Bob used the same bases is plotted in two

Table 1. *Experimental quantum key distribution results*

distance (km)	$\bar{n}$	bit-error rate (%)	received bit rate (s^{-1})
10.8	0.1	1.5	700
10.8	0.2	1.2	1400
21.8	0.1	4	350
21.8	0.2	2.8	700
30	0.2	4	260

halves: figure 3*a* shows the received data for the bit periods when Alice sent a 0, and figure 3*b* shows the data obtained when Alice sent a 1. It can be seen that the error rate is relatively low. Table 1 shows the bit rates and bit error rates obtained for many such transmissions over distances of 10.8, 21.8 and 30 km, and using $\bar{n}$ values of 0.1 and 0.2. The most important parameter here is the error rate, which must be as small as possible when there is no eavesdropper present on the channel. The experimental values, which range from 1.2–4%, are sufficiently low for Alice and Bob to recover error-free secret keys in each case (Marand & Townsend 1995) using secure error-correction and privacy amplification techniques (Bennett *et al.* 1988, 1992*a*). For the 10.8 km distance we obtain transmission rates in the 1 kbit s^{-1} range; however, we have also demonstrated the feasibility of using a higher frequency source in the system, in which case the transmission rate over the same distance was $\sim$ 20 kbit s^{-1} (Townsend 1994). Currently, the performance of the system is limited by the properties of the germanium APD detector. As single-photon detector technology for the 1.3 and 1.5 μm wavelength regions improves, both transmission distances and bit rates are likely to increase.

4. Short-span point-to-point quantum key distribution

(*a*) *Introduction*

The second prototype quantum cryptography system that we shall discuss is designed to operate at shorter wavelengths around 0.8 μm in order to exploit the superior performance of silicon APD detectors. At this wavelength the fibre has relatively high values of loss $\sim$ 2 dB km^{-1} and GVD ~ -90 ps nm^{-1} km^{-1}; however, this is not necessarily a problem for short-span applications. A potentially more serious issue arises from the fact that standard fibre supports multiple spatial modes for wavelengths shorter than about 1.2 μm. For conventional communication systems this is highly undesirable since modal dispersion and modal beat-noise can seriously degrade both the maximum achievable bit rate and the bit-error rate in the system. In a polarization-encoded quantum cryptography system, an additional problem may arise from the fact that the polarization states of the various modes can evolve at different rates during propagation, and this can also lead to increased error rates. To the best of our knowledge, other workers in the field (Muller *et al.* 1993; Franson & Ilves 1994; Franson & Jacobs 1995) using wavelengths shorter than 1 μm in their systems have either employed non-standard fibre that is single moded at their operating wavelengths, or have not explicitly addressed the issue of multimode propagation.

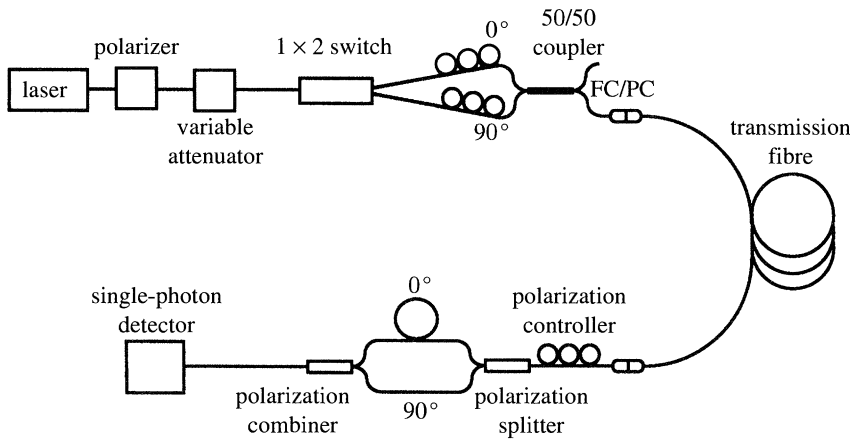

Figure 4. Prototype polarization-encoded quantum cryptography system.

The use of non-standard fibre can be a serious practical limitation, however, since a large fibre infrastructure designed for 1.3–1.5 μm operation already exists, and fibre that is single moded at shorter wavelengths tends to exhibit excessive bend loss at one or both of these wavelengths and, hence, is unsuitable for general applications. As a consequence, we have investigated the feasibility of quantum key distribution in the multimode regime of standard fibre.

(*b*) *Prototype polarization-encoded system*

The experimental set-up is illustrated in figure 4. The source is a 0.83 μm-wavelength semiconductor laser which is gain switched at 1 MHz to produce a train of 300 ps-long optical pulses. The average photon number and polarization state of each pulse entering the transmission fibre are controlled by means of a calibrated variable attenuator and an optical switch that is followed by a pair of static polarization controllers. The 1-into-2 switch is based on an acousto-optic modulator that is modified to achieve a high on : off ratio of $\sim$ 1000 : 1 at its output ports. The transmission link is a drum of standard telecommunications fibre that is connected into the experiment using commercial FC–PC connectors. At 0.83 μm the fibre loss is about 2 dB km^{-1}. Pulses exiting the fibre are detected using a polarization-sensitive time-correlated photon-counting set-up (Townsend *et al.* 1993*a*) based on a silicon APD (EG&G SPCM100) which has a quantum efficiency of 27% at 0.83 μm and a very low dark-count rate of $\sim$ 50 s^{-1}. Apart from the transmission fibre, all components in the experiment have fibre pigtails that support a single spatial mode at the operating wavelength.

At 0.83 μm the transmission fibre has a normalized frequency or V-number of 3.4 and is therefore able to support two spatial modes, namely LP_{01} and LP_{11} (Gloge 1971). The relative coupling to these modes was investigated by exploiting the effects of modal dispersion in the fibre to temporally separate the two spatial components. For this experiment, only one of the possible input polarizations was used and the polarization splitter–combiner pair in front of the detector was removed. The average photon number, $\bar{n}$, for the optical pulses at the input to the fibre was 0.1 and a long 8.2 km fibre was used to achieve a large mode separation. The upper trace in figure 5 shows the measured photocount distribution, which consists of two peaks separated by 11.4 ns. The x-axis represents the time interval between a photodetection and

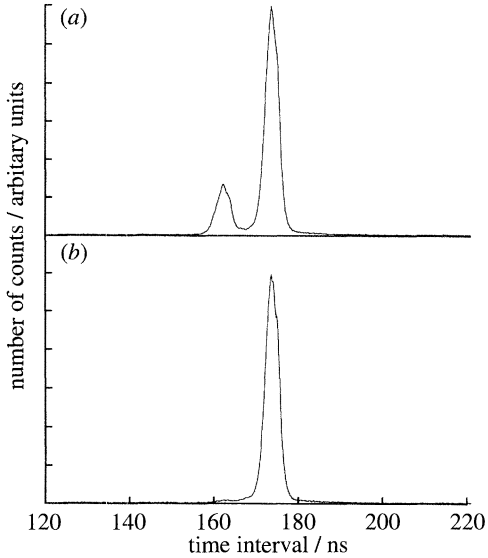

Figure 5. Photocount distribution obtained after propagation through 8.2 km of fibre. The upper trace (*a*) shows two peaks separated by 11.4 ns, which arise from dispersion of the LP_{01} and LP_{11} modes. The lower trace (*b*), which was obtained with a spatial-mode filter at the input to the fibre, shows only the LP_{01} peak.

the next laser drive pulse that follows in time. Hence, photons that generate the larger peak arrive at the detector earlier than those that generate the smaller peak. For an 8.2 km-long step index fibre with $V = 3.4$, we calculate that the LP_{11} mode should lag the LP_{01} mode by 10 ns (Gloge 1971). This is in good agreement with the experimentally observed time delay, and identifies the larger peak as the LP_{01} fundamental mode. Since the LP_{11} mode has a larger fraction of power propagating in the cladding compared to the LP_{01} fundamental, it is more susceptible to bend-induced radiation loss. We make use of this fact to create a simple spatial mode filter by inserting 3–4 small loops into the transmission fibre immediately following the FC–PC connector at the input. This process has the effect of removing the LP_{11} peak from the photocount distribution (lower trace in figure 5), which shows that the coupling into this mode occurs only at the input FC–PC connector and not during propagation through the fibre. Furthermore, no evidence of coupling into the LP_{11} mode was found when the fibre contained fusion-spliced joints, or when the fibre was subjected to a large thermal strain by blowing hot air onto one side of the fibre drum for several hours.

Having obtained true single-spatial-mode propagation, we used the system to investigate the transmission of polarization-encoded data at the single-photon level. In this case, the system was configured as shown in figure 4, and the fibre length was reduced to 1 km in order to reduce the effects of both chromatic dispersion and polarization mode dispersion (Breguet *et al.* 1994). The polarization controllers in the transmitter were adjusted so that the $\bar{n} = 0.1$ pulses at the fibre input were linearly polarized at either 0° and 90° to an arbitrary reference frame. During transmission, the polarization state of the pulses evolves due to birefringence in the fibre, which arises from factors such as core ellipticity and bend-induced stress. This was compensated for in the experiment by adjusting the polarization controller in the receiver to linearize the output from the fibre and match the 0° and 90° states to the reference

frame of the polarization splitter. In the current prototype only one polarization basis was used, comprising the two orthogonal 0° and 90° linear polarization states which represent the binary digits 0 and 1, respectively. Consequently, the system could not be used for secure key distribution based on the original protocol (Bennett *et al.* 1983, 1992*a*) since this requires the use of a second non-orthogonal polarization basis and, hence, additional modulators. However, bit- and bit-error-rate information for the single-basis transmission of random bit sequences provides a good indication of the complete system performance. In this case, we find bit-error rates of $\sim 1.1\%$ and bit rates of ~ 8.3 kbits s^{-1}. The error rate in the system is currently limited by the accuracy with which the polarization controllers, which are designed for optimum operation at a different wavelength, can set the linear polarization states. The extinction ratio for the polarization splitter is 24 dB, which suggests that an error rate of 0.4% should ultimately be attainable. Most importantly, detector dark counts only contribute about $10^{-3}\%$ to the observed error rates, so the system can tolerate significantly more loss before error-rate performance is degraded. This contrasts with the system described in § 3, which is loss limited in the sense that dark counts from the germanium APD provide one of the dominant contributions to the observed error rate. These results suggest that, in the future, systems based on silicon APDs could be used for secure key distribution in short-span point-to-point links or small local area networks. As we shall describe below, the latter application requires a large effective increase in system loss due to the presence of optical splitters in the quantum channel. Consequently, due to their low dark-count rates, silicon APDs are well suited for this type of application.

5. Quantum cryptography on passive optical networks

To realize the true potential of quantum cryptography, it is important that the technique can be implemented on networks. In this case, communications of the type any-to-any and any-to-many can occur, in contrast to the 'conventional' application of one-to-one key distribution between a single transmitter and receiver pair. We have developed several techniques that allow multiuser operation to be achieved on fibre-distributed networks by means of simple adaptations of the original protocols and equipment configurations (Townsend *et al.* 1994*b*; Phoenix *et al.* 1995). The schemes allow Alice, who now plays the role of network controller, to distribute distinct secret keys to each of N Bobs on the network, and, hence, to securely encrypt and authenticate subsequent data transmissions broadcast on the network.

An optical network is a basic requirement for quantum key distribution, since the technique exploits the properties of photons. We consider first tree and star networks, of the type shown in figure 6*a*, in which the nodes are passive optical splitters; however, other architectures such as bus or ring networks could also be employed. The internal structures of the controller and terminals are not shown explicitly, since they can be identical to those of the transmitters and receivers already discussed in the point-to-point schemes. A defining feature of such passive optical networks (PONs) is that, in contrast to circuit switched networks, broadcast-mode communications are possible. This is due to the classical behaviour of multiphoton signals at the network nodes, which ensures that all downstream terminals on the network receive identical copies of messages broadcast by the controller or exchange at the head-end of the PON. Similarly, for upstream communications, the controller can 'broadgather' messages from all the individual terminals on the network.

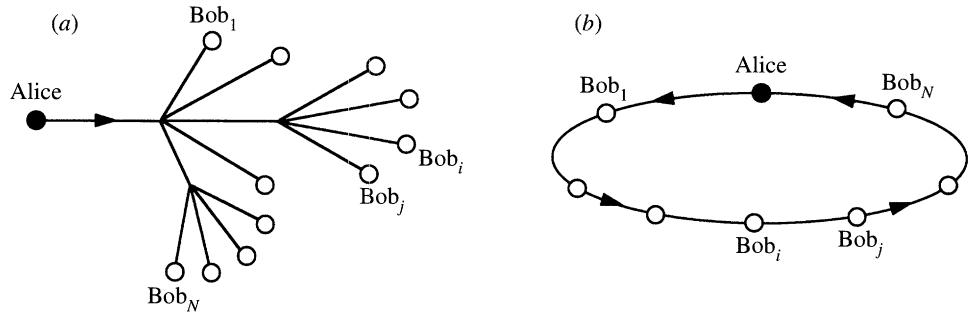

Figure 6. Optical fibre-based network architectures: (*a*) tree and star; (*b*) looped.

The implementation of quantum key distribution on such a network is remarkably straightforward, since it mainly requires a simple exploitation of the properties of low-intensity quantum fields at the network nodes. For example, the basic laws of quantum mechanics dictate that single quanta, such as photons, can neither be split nor cloned (Wootters & Zurek 1982). Therefore, if Alice sends a randomly encoded sequence of single photons into a multiterminal network containing a sequence of couplers, a given input photon (and hence the bit that it represents) can only ever reach a single receiver, not multiple receivers. The same is true, except with small probability, when optical pulses with average photon number $\bar{n} \ll 1$ are used. In order to implement the standard quantum cryptography protocols on the network, Alice transmits a randomly encoded sequence of clocked pulses into the network, and all the Bobs simultaneously make synchronous but independent random measurements on the network outputs. Because of the statistically random output from each coupler, this procedure is equivalent to simultaneously setting up N distinct quantum cryptography links in which Alice sends a different random sequence in each case. Of course, Alice does not know in advance which Bob will receive a given pulse; however, this is taken care of in the public discussion phase of the protocol during which she sequentially polls each Bob on the network and performs a temporal correlation of the sent and received data, as in the point-to-point case discussed earlier. At the end of the process, Alice has established a distinct sequence of secret bits with each terminal Bob_i on the network, which is used for authentication (Bennett & Brassard 1985) and the generation of a shared key K_i. If required, Alice can then use the individual K_i as keys in one-time pad encryptions of a master network key or keys. The latter can then be securely distributed to all Bobs, or subsets of Bobs, on the network. Consequently, two types of encrypted communication are enabled. In one-to-one communications, Alice uses K_i to encrypt data signals intended only for Bob_i. Hence, although these signals are broadcast on the network and are therefore accessible to all Bobs, only Bob_i can decode the data. In this scenario, secure inter-Bob communications can still take place, but Alice must act as an interpreter. Any-to-any communications can also take place among subsets of Bobs sharing a master key, and in this case Alice performs only a routing function.

Quantum cryptography can also be employed on other types of network architecture, such as that shown in figure 6*b* in which there is a looped optical path returning to Alice, who now plays the role of transmitter and receiver on the network. In contrast to the previous schemes, each Bob modulates (e.g. polarization modulation), but does not destructively measure, the photons circulating around the network. Single-photon detection equipment, of the type used in the point-to-point scheme,

is now only located in Alice the network controller. A similar looped network could also be realized with the branched architecture shown in figure 6*a* if the terminals are supplied with reflective modulators. Whilst these simple network architectures are useful for demonstrating the basic concept of a quantum cryptography channel comprising N-modulators, they are, however, vulnerable to certain types of eavesdropper attack. This topic is discussed in detail elsewhere (Phoenix *et al.* 1995), and here we simply mention the functionalities that can be achieved with the simple model network. These include sequential key distribution from Alice to each Bob on the network (Townsend *et al.* 1994*b*), but also an important new mode of operation that allows any pair of users Bob_i and Bob_j to establish a shared secret key that is not known to Alice (Phoenix *et al.* 1995). In the latter case, Alice circulates photons around the network and Bob_i and Bob_j perform random modulations on this sequence. After the transmission, Alice publishes the results of her measurements and, from a knowledge of his own modulator settings, Bob_i can then calculate the settings of Bob_j and vice-versa. In this way, Bob_i and Bob_j can establish a key that is not known to Alice. This is very important, since it means that the network provider facilitates, but does not have access to, confidential communications between users of the network.

6. Conclusions

In summary, we have discussed some of the important issues that influence the design of optical-fibre-based quantum cryptography systems. Point-to-point schemes for both the first and second telecommunication windows have been investigated, and secure key distribution demonstrated over distances up to 30 km. We have also described techniques that allow quantum cryptography to be used on optical networks with many users. There are a wide range of applications for such network architectures, including, for example, optically distributed computer LANs, local-access telecommunications networks, and cable-television distribution networks. In the future, quantum cryptography may play an important role in providing high levels of security in these areas.

References

Bennett, C. H. 1992 Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124.

Bennett, C. H. & Brassard, G. 1985 Quantum public key distribution system. *IBM Technical Disclosure Bulletin* **28**, 3153–3163.

Bennett, C. H., Brassard, G., Breidbart, S. & Wiesner, S. 1983 Quantum cryptography or unforgeable subway tokens. In *Advances in Cryptology: Proc. Crypto'82* (ed. D. Chaum, R. L. Rivest & A. T. Sherman), pp. 267–275. New York: Plenum.

Bennett, C. H., Brassard, G. & Robert, J.-M. 1988 Privacy amplification by public discussion. *SIAM Jl Comput.* **17**, 210–229.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. 1992*a* Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28.

Bennett, C. H., Brassard, G. & Ekert, A. E. 1992*b* Quantum cryptography. *Scient. Am.* October, 26–33.

Breguet, J., Muller, A. & Gisin, N. 1994 Quantum cryptography with polarised photons in optical fibres. Experiments and practical limits. *J. Mod. Opt.* **41**, 2405–2412.

Ekert, A. E. 1991 Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Ekert, A. E., Rarity, J. G., Tapster, P. R. & Palma, G. M. 1992 Practical quantum cryptography based on two-photon interferometry. *Phys. Rev. Lett.* **69**, 1293–1295.

Franson, J. D. & Ilves, H. 1994 Quantum cryptography using optical fibres. *Appl. Opt.* **33**, 2949–2954.

Franson, J. D. & Jacobs, B. C. 1995 Operational system for quantum cryptography. *Electron. Lett.* **31**, 232–234.

Gloge, D. 1971 Weakly guiding fibers. *Appl. Opt.* **10**, 2252–2258.

Lacaita, A., Cova, S., Zappa, F. & Francese, P. A. 1993 Subnanosecond single-photon timing with commercially available germanium photodiodes. *Opt. Lett.* **18**, 75–77.

Marand, C. & Townsend, P. D. 1995 Quantum key distribution over distances up to 30 km. *Opt. Lett.* **20**, 1695–1697.

Muller, A., Breguet, J. & Gisin, N. 1993 Experimental demonstration of quantum cryptography using polarised photons in optical fibre over more than 1 km. *Europhys. Lett.* **23**, 383–388.

Owens, P. C. M., Rarity, J. G., Tapster, P. R., Knight, D. & Townsend, P. D. 1994 Photon counting with passively quenched germanium avalanche photodiodes. *Appl. Opt.* **33**, 6895–6901.

Phoenix, S. J. D., Barnett, S. M., Townsend, P. D. & Blow, K. J. 1995 Multi-user quantum cryptography on optical networks. *J. Mod. Opt.* **42**, 1155–1163.

Townsend, P. D. 1994 Secure key distribution system based on quantum cryptography. *Electron. Lett.* **30**, 809–811.

Townsend, P. D., Rarity, J. G. & Tapster, P. R. 1993*a* Single photon interference in a 10 km long optical fibre interferometer. *Electron. Lett.* **29**, 634–635.

Townsend P. D., Rarity J. G. & Tapster, P. R. 1993*b* Enhanced single photon fringe visibility in a 10 km long prototype quantum cryptography channel. *Electron. Lett.* **29**, 1291–1292.

Townsend, P. D., Phoenix, S. J. D., Blow, K. J. & Barnett, S. M. 1994 Design of quantum cryptography systems for passive optical networks. *Electron. Lett.* **30**, 1875–1876.

Walker, N. G. & Walker, G. R. 1990 Polarisation control for coherent communications. *J. Lightwave Tech.* **8**, 438–458.

Wooters, W. K. & Zurek, W. H. 1982 A single quantum cannot be cloned. *Nature* **299**, 802–803.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES