JOURNAL OF MODERN OPTICS, 2001, VOL. 48, NO. 13, 1957–1966

Eighty kilometre transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm

PHILIP A. HISKETT†, GABRIELE BONFRATE‡, GERALD S. BULLER† and PAUL D. TOWNSEND‡

†Department of Physics, Heriot-Watt University, Edinburgh, UK, EH14 4AS; e-mail P.A.Hiskett@hw.ac.uk

‡Corning Research Centre, Ipswich, UK, IP5 5RE

(*Received 16 February 2001; final version received 23 July 2001*)

Abstract. A polarization-based receiver for quantum key distribution incorporating an InGaAs/InP single photon avalanche photodiode (SPAD) has been constructed to investigate the potential for increasing the transmission distance in long wavelength quantum key distribution systems beyond the 50 km range.

1. Introduction

As computer networks and the need for secure data transmission grow, cryptography is assuming an increasingly important role. It enables the users of a communication channel to secretly exchange messages even in the presence of eavesdroppers. This is achieved by encrypting the data using a key known only to the legitimate parties. It is apparent that the security of the system relies on the secrecy of the shared key. However, any classical key distribution system suffers from the weakness that the key, at least in principle, can be copied during distribution without alarming the parties involved. Quantum Key Distribution (QKD) systems enable the sender (Alice) and the receiver (Bob) to generate and distribute a verifiably secure key over a communication channel, even under the attack of an eavesdropper (Eve) [1–3]. The security is guaranteed by fundamental principles of quantum mechanics, such as complementarity and/or non-locality. To date there have been several demonstrations of QKD, in which the key is encoded on pairs of non-commuting observables, typically phase or polarization states of single photons or weak coherent optical pulses (the practicalities of how the key is encoded have been described in detail in [3–7]). Prototype quantum cryptography systems incorporating germanium single photon avalanche diode (SPAD) detectors and using silica optical fibres to transmit the photons, have been constructed and QKD over distances of 50 km have been realized at a wavelength of 1.3 μm [4].

The potential range of such systems is limited by the high attenuation of 1.3 μm wavelength photons in optical fibres (~0.3–0.4 dB/km). In order to increase the range of QKD systems the third transmission window of silica optical fibres (~0.2–0.25 dB/km) at around 1.5 μm must be targeted. At this wavelength the

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online © 2001 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/09500340110085112

main practical issue concerns the lack of efficient, low noise single-photon detectors. Germanium SPADs require operation at cryogenic temperatures to reduce thermally generated counts, this cooling shifts the absorption band-edge sufficiently that the detection efficiency of such SPADs at 1.55 μm is reduced to, typically, $\ll$1%. In contrast InGaAs/InP SPAD detectors [8, 9] have been shown to be the most promising candidate for detection of single photons at a wavelength of 1.55 μm and prototype quantum cryptography systems incorporating such devices have been constructed [7]. The receiver described in this paper is for potential use in a full QKD system in which randomly produced bit values are encoded onto weak coherent pulses by way of polarization. In this paper, which describes the characterization of a QKD receiver and not a full quantum cryptography system, the bit value, i.e. polarization of the weak coherent pulses was kept constant, so that the performance of the receiver could be characterized under realistic system conditions with the aim of maximizing the achievable transmission distance in QKD. Since the full QKD protocol with dynamic polarization modulation was not implemented no data sifting and privacy amplification were required.

2. Operating conditions of the SPAD detector

The detector used in this system was a 40 μm diameter pigtailed InGaAs/InP SPAD (Epitaxx model EPM239SAA) operated in gated mode. This operating technique, where the SPAD is DC biased at just below the breakdown voltage and periodically brought above breakdown for a short time by applying an AC gate pulse (this AC gate pulse is time-correlated to the arrival of the single photons) has been extensively described in the literature [10, 11].

In order to assess the performance of the receiver the SPAD was operated at a temperature of 140 K in gated mode. The SPAD was DC biased at 1V below the breakdown voltage while the AC gate pulse of 4V caused the SPAD to reach an excess bias of 3V. At this temperature and excess bias the instrumental response time was measured to be 265 ps full-width-at-half-maximum (FWHM). If a stable optical source is used and the gate pulse applied to the SPAD is accurately time-correlated to the arrival of the single photons, it is usually only necessary to consider counts that occur in a time window within the gate equivalent to the instrumental response of the device at the time interval where the single photons are expected to be incident on the SPAD. Any counts that occur outside this window will not be considered as photocounts (i.e. bits). To ensure the full excess bias was reached for the necessary 265 ps, the length of the gate pulse was chosen to be 3.5 ns. The gate pulse could not be shortened any further because the RC time constant of the device did not allow the full excess bias to be applied to the device for a time of 265 ps. With a 3.5 ns gate it was possible to operate the SPAD at 100 kHz gating rate. Although the dark count rate at 140 K is significantly higher than the corresponding value at lower temperatures because of the increased number of thermally induced dark counts, the after-pulse probability is greatly reduced, as the filled traps emit carriers more rapidly. At an excess bias of 3V and a temperature of 140 K, the detection efficiency and dark count probability per gate within a time period equivalent to the 265 ps instrumental response time of the device were measured to be 12.16% and 1.6×10^{-6}, respectively.

3. System experiments: method and results

The timing of a QKD system is vital when using the gated mode technique because single photons must arrive at the SPAD precisely when it is biased above breakdown, i.e. synchronous to the gate pulse. In addition, the timing pulse in the system allows Alice and Bob to 'time stamp' each transmitted and received bit so that in the post-transmission public discussion they can sift their raw data to generate a shared key. For the receiver discussed in this paper, two different approaches towards the achievement of system timing and synchronization were explored: wavelength division multiplexing (WDM) and spatial multiplexing.

3.1. *WDM*

The WDM based system (figure 1) employed 40 km of dispersion shifted optical fibre (Corning DS).

Two gain-switched, distributed-feed-back (DFB) lasers emitting 100 ps pulses at 100 kHz repetition rate were used in the system: a 1.55 μm wavelength 'signal' DFB attenuated to an average 0.1 photons per optical pulse and a synchronously triggered 1.3 μm wavelength 'clock' DFB for timing purposes. For experimental convenience the two lasers were driven by a single electrical pulse source. This had the advantage of ensuring low relative timing jitter between the signal and clock pulses, but the disadvantage that the clock pulses were shorter than optimum for the clock receiver. The frequency of the 1.55 μm weak signal pulse was reduced by a factor of two by using an amplitude modulator to remove each alternate pulse. For each 1.55 μm weak signal pulse, therefore, there were two accompanying 1.3 μm clock pulses (see later). A combination of WDM couplers and filters was used to combine and separate the two optical pulses at the transmitter and receiver ends of the system respectively.

At the receiver end of the system a germanium APD, biased at 95% of the breakdown voltage, was used to detect the arrival of the timing pulse. However, the sensitivity and bandwidth (≈1 GHz) of the available APD and associated detection electronics were found to be too low for efficient detection of unamplified

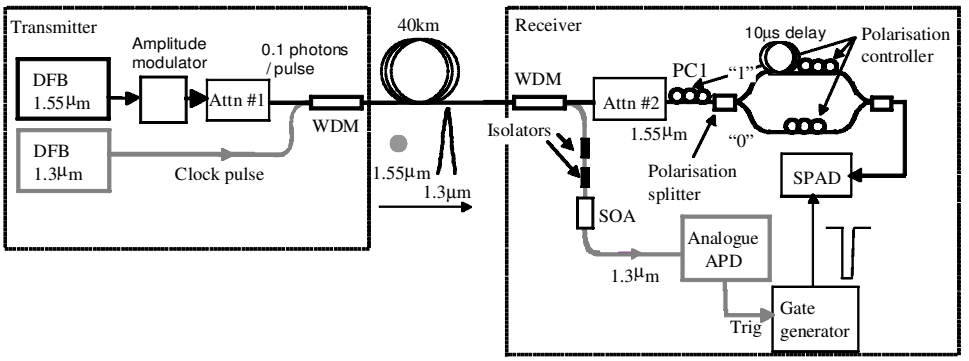

Figure 1. Forty kilometres WDM-based receiver used to predict the QBER of a QC system containing the InGaAs/InP SPAD. The laser pulse from the 1.55 μm wavelength DFB is attenuated (by Attn#1) so that on average 0.1 photons per pulse will be launched into the 40 km optical fibre. The increase in length of optical fibre can be simulated by increasing the attenuation at the second attenuator (Attn#2). The clock pulse in the system is a 1.3 μm wavelength pulse from a DFB laser.

clock pulses. This resulted from the relatively high fibre attenuation at 1.3 μm (16 dB in total over 40 km) and the shorter than ideal duration of the clock pulses (100 ps). A semiconductor optical amplifier (SOA) was therefore used to increase the clock pulse power to a detectable level. In order to limit the amount of amplified spontaneous emission (ASE) from the SOA reaching the SPAD two optical isolators were placed in series between the SOA and the WDM.

The receiver also contains a polarization splitter/combiner network incorporating a fibre delay in one channel. The initial polarization controller (PC1 in figure 1) in the polarization splitter/combiner network allowed correction of any drift in the polarization of the weak signal pulse that will have occurred as the pulse was transmitted through the fibre. In a practical system this polarization controller would need to be automated and actively controlled to maintain the alignment of the polarization reference frames of the transmitter and receiver. However, for the purposes of the characterization reported here the polarization drift was sufficiently slow that manual alignment could be employed (typical stability period ~30 minutes). The fibre delay incorporated in one channel of the network has the effect of introducing a relative time delay between orthogonally polarized input pulses. This allowed a significant simplification of the receiver apparatus since a single SPAD (rather than two) is used to detect and differentiate between (by means of time delay) the orthogonal polarization states. In detail the timing scheme works as follows: upon detection of the 1.3 μm wavelength clock pulse a gate generator applied a voltage pulse to the SPAD to bias it above breakdown. Note that the transmitter generates two clock pulses (10 μs period) for each weak 1.55 μm signal pulse (20 μs period). The weak signal pulse, depending on its polarization, is directed via the polarization splitter/combiner network either directly to the SPAD or to the SPAD via the 10 μs fibre delay (see figure 2). Hence the timing of the system was arranged so that the 1.3 μm clock pulse caused the SPAD to be biased above breakdown synchronous to the two possible time windows in which the 1.55 μm weak signal pulse could reach the SPAD. The polarization, and hence the bit values, were distinguishable by determining the time window in which the weak signal pulse was detected.

In order to estimate the quantum bit error rate ratio (QBER) of this system, the polarization of the weak signal pulse was chosen to be the same for each pulse, e.g. only '0' bits would be transmitted. At the start of the measurement, the polariza-

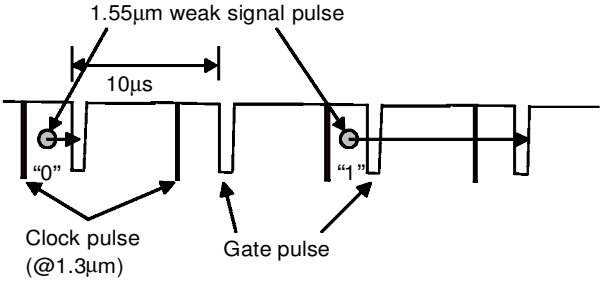

Figure 2. Schematic of gating arrangement used in the InGaAs/InP SPAD based receiver for quantum key distribution. The weak signal pulse, depending on its polarization, will be delayed or sent directly through to the SPAD. The delay is chosen so as to match the period of the 1.3 μm clock pulse train.

tion controller immediately before the polarization splitter/combiner network (PC1 in figure 1) was adjusted to maximize the transmission in the channel of the network corresponding to the bit value sent by the transmitter, e.g. if only '0' bits were being transmitted, the polarization controller would be adjusted to maximize the signal transmitted through the '0' channel of the network, therefore maximizing the count rate in the non-delayed gate pulse of the SPAD. In a perfect system, Bob would receive counts only in the gate pulse corresponding to the non-delayed photons because Alice only sends '0' bits. However, the non-100% extinction ratio of the polarization splitter and the dark counts and afterpulsing of the SPAD itself will cause some counts to be registered in the time window associated with the orthogonal polarization. This leads Bob to record a '1', i.e. an error. A good estimate of the QBER that would be observed in a complete system can therefore be obtained from the quantity $[C_1/(C_0 + C_1)]$, where C_1 is the count rate in a time window equivalent to the instrumental response time of the SPAD (i.e. 265 ps) within the '1' gate and C_0 is the count rate in a time window equivalent to the instrumental response time of the SPAD within the '0' gate. Similarly a further QBER estimate can be obtained from $[C_0/(C_0 + C_1)]$ in the case where only the input state of '1' is transmitted. Since the QBER value determines the security and efficiency of QKD it is important to evaluate this parameter as a function of distance in order to determine possible operating limits. In the experiment additional fibre lengths were simulated by incorporating a fibre attenuator into the receiver (Attn#2).

The measured count rates C_1 and C_0 of this 40 km based system and the values obtained for larger simulated distances are shown in figure 3.

The observed behaviour can be explained as follows: as the average number of photons emerging from Attn#2 is reduced, the probability of a photodetection event in the correct ('0') gate pulse decreases and so does the probability of an after-pulse in following ('1') gate pulse. Hence C_1 and C_0 both decrease proportionally with increasing distance. At very high levels of attenuation (i.e. long simulated fibre distances) the photodetection probability is small and hence the afterpulsing probability in a following gate becomes negligible compared to the probability of a dark count caused by tunnelling or thermally excited carriers. Hence C_1 and C_0 both begin to converge towards the dark count rate at high attenuation. However, from figure 3, it is clear that the value of C_0 tends to $\sim 0.17\,\mathrm{cs}^{-1}$ at long fibre distances. This count rate is slightly higher than the expected dark count rate of $0.08\,\mathrm{cs}^{-1}$ (calculated from the product of the probability of dark count per gate, 1.6×10^{-6} and the repetition rate of the gate pulse corresponding to the '0' bits, 50 kHz). The higher count rate was determined to be caused by a very small amount of ASE from the SOA reaching the SPAD. The QBER values calculated from the values of C_0 and C_1 are shown in figure 4. An additional point obtained using a 51 km reel of fibre is also shown that confirms the 4% value obtained by simulating this distance. It was not possible to increase the transmission fibre length in the WDM experiment further because the sensitivity of the available clock receiver was too low to tolerate the additional transmission loss. However, this limitation is not intrinsic and the WDM technique appears to be quite promising for achieving low-jitter clock delivery in a gated-mode, long distance QKD system.

The maximum tolerable value of background error rate and the maximum achievable transmission distance in practical QKD systems have been the subject

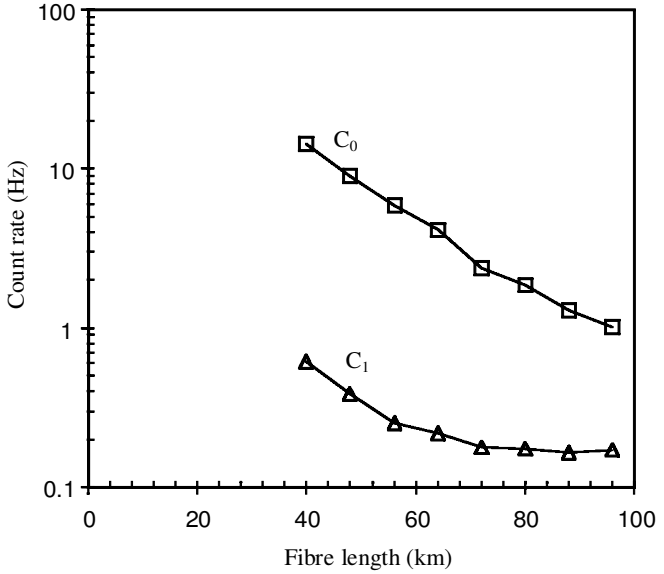

Figure 3. Graph of count rate C_0 and C_1 against fibre length.

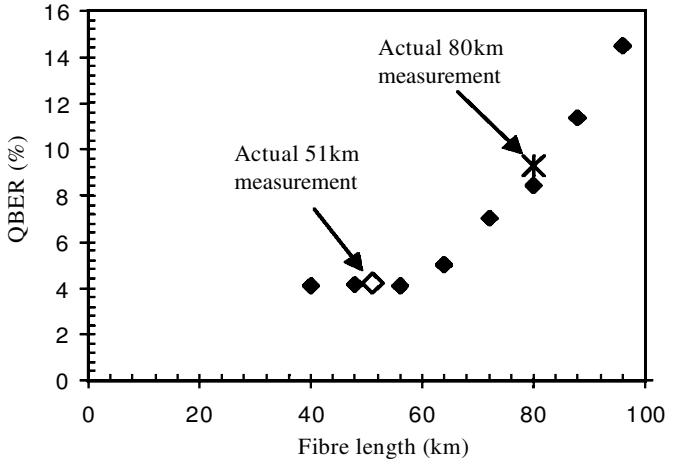

Figure 4. Graph of QBER against fibre distance. The main curve was taken for a 40 km WDM-based system and the extra fibre lengths simulated by using a second attenuator. The 40 km fibre reel was replaced by a 51 km and 80 km reel and the QBER was measured at these two actual distances. The 80 km fibre reel was used in the spatial multiplexing system.

of a great deal of recent research activity (see [12] and references therein). While a full discussion of this work is beyond the scope of this paper the broad issues can be briefly reviewed as follows. After the initial transmission process Alice and Bob must sift their raw bit sequence retaining only the bits where Bob obtained a deterministic outcome (half the bits on average). At this point Alice and Bob are in possession of a shared random bit sequence that contains a relatively small fraction of errors (the number of errors that would be expected in a system based on the

current receiver design can be estimated directly from the measured QBER values). Alice and Bob can now employ error correction techniques to remove the errors from their shared bit sequences [2, 12]. At this stage the bit sequences are error-free, but possibly only partially secret because of potential information leakage to an eavesdropper. This possibility arises from the non-zero error rate and from other non-idealities in the system such as, for example, the small fraction of multi-photon pulses generated by Alice if she uses an attenuated coherent source. In order to recover from this potential insecurity Alice and Bob must employ a classical hashing technique known as privacy amplification to reduce any information obtained by an eavesdropper to an arbitrarily small fraction of a single bit leaving them with a final, error-free and certifiably-secret, key [13]. However, the privacy amplification process involves a shortening of the shared bit sequence, so if the information leakage on the QKD channel is too high the effective transmission rate for secret bits can be zero [12]. In any real application of QKD a risk assessment process would be used to select an allowable operating range in which the theoretical security risks are balanced against practical issues such as system cost and complexity. Nevertheless, it is possible to make some general statements concerning security of practical systems. As shown in [12], in an ideal QKD system employing single photon signals the transmission rate for secret bits is non-zero for QBER values less than about 11%. However, in real systems with loss and non-ideal sources the QBER requirements and distance limits can be more restrictive [12]. Here we restrict ourselves to a general observation based on [12] that the security of the current system would be optimized with the use of a parametric downconversion source rather than the attenuated coherent source used in the experiments.

3.2. *Spatial multiplexing*

An alternative approach to the system design is to use two separate optical fibres to carry the clock and signal pulses (Spatial Multiplexing). This scheme has the advantage of removing the problem of channel isolation as the high power clock channel can be confined to a fibre that has no optical connection to the SPAD. However, in a real system the spatial multiplexing scheme may also have a number of disadvantages. The first and most obvious issue is that twice as many fibres are needed for the QKD system and this has implications as far as the system cost is concerned. Perhaps more importantly, the system may be unstable if the two fibres experience differential temperature fluctuations because the separation between clock and signal pulses will vary with time. In order to investigate this issue and to make comparison with the WDM technique a second version of the experiment was used in which the clock channel wavelength was changed to 1.55 μm and the clock pulse was transmitted over a separate fibre (i.e. spatial multiplexing) see figure 5.

As with the WDM-based system, the 1.55 μm DFB laser was operated at 100 kHz and an amplitude modulator was used to remove each alternate pulse from the transmission line. The frequency of the clock pulses sent down the clock line remained at 100 kHz. The pulses from the clock line were amplified using an Erbium-doped fibre amplifier (EDFA) and were now detected by a HP Lightwave Converter rather than the cooled germanium APD. The system also contains the polarization splitter/combiner network from the WDM system. The same method employed to determine the QBER of the WDM system was used for this system,

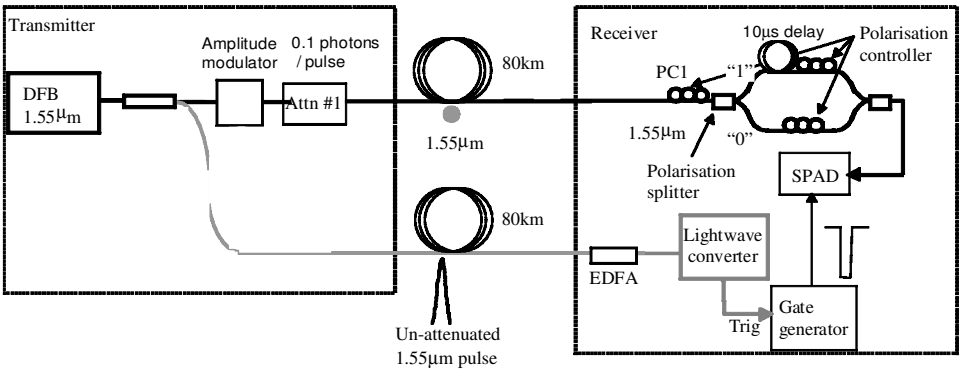

Figure 5. Eighty kilometres spatial multiplexing-based receiver used to predict the QBER of a QC system containing the InGaAs/InP SPAD. The laser pulse from the 1.55 μm wavelength DFB is split into the two 80 km fibres. In one fibre the pulse is attenuated (by Attn#1) so that on average 0.1 photons per pulse will be transmitted. In the other fibre, the pulse was amplified by an EDFA and used as a clock pulse in the system.

i.e. photons of only one polarization state were transmitted to Bob. Bob, once again, uses his polarization controller (PC1 in figure 5) to maximize the signal in the channel of the polarization splitter/combiner network corresponding to the polarization sent by the laser source.

In this system the clock receiver did not limit performance of the system and the transmission distance could then be increased to 80 km and the QBER measurement repeated. As shown in figure 4 this result of QBER = 9% is in good agreement with the predicted values obtained using optical variable attenuators, confirming both a low level of cross-talk in the WDM scheme and negligible dispersion penalties at the increased 80 km transmission distance in the spatial multiplexing scheme. The results confirm the potential for increasing the transmission distance to the 80 km range in QKD systems based on InGaAs/InP SPADs.

4. Stability

Thermal instabilities can cause fluctuations in the refractive index and the effective length of the optical fibre used in both systems. The rate of change of refractive index with temperature for optical fibre is typically $\sim 1 \times 10^{-5}\ \mathrm{K}^{-1}$ [14]. This change of refractive index is potentially less of a problem with the WDM system because both clock and signal are transmitted through the same fibre, however, the change in refractive index will differ slightly for the two wavelengths. The thermal stability of the WDM-based system was investigated by heating the 40 km reel of optical fibre to 40°C and then monitoring the drift and walk-off of the 1.3 μm and 1.55 μm pulses. The heating caused the position of both pulses to drift in time, however, no significant relative walk-off was observed and, therefore, the timing of the system was preserved. For the case of the spatial multiplexing system, where clock and signal are transmitted through separate fibres, a fluctuation in the relative temperature between the clock and signal fibre will cause relative temporal walk-off between the two pulses. Taking the example of a system

containing two 80 km reels of optical fibre where there is a relative temperature change of 1°C between the two fibres, the separation of clock and signal would be ~2.6 ns. This is significant as it is comparable to a gate width, however, the problem could easily be solved by using a slow tracking circuit to keep the gate synchronized to the signal.

5. Conclusion

The performance of a 1.55 μm, InGaAs/InP SPAD-based receiver for quantum key distribution has been investigated experimentally. Two different approaches were used to separate and isolate the clock and signal channels in the system, the first was based on a WDM technique over a single transmission fibre and the second employed spatial multiplexing over a pair of fibres. For fibre lengths of 40 km and 51 km the error rate of the WDM-based system was found to be dominated by afterpulses in the SPAD and a QBER value of 4% was obtained at both distances. Longer transmission distances were also simulated in the WDM configuration by adding attenuation to the system. The results showed that the 4% QBER value was maintained for distances up to 60 km. For longer simulated distances the QBER increased due to the effect of detector dark counts reaching a value of about 9% at 80 km. Subsequent experiments using a pair of 80 km-long fibres in the spatial multiplexing configuration also gave a QBER of 9% at this distance. Stability tests showed that without any external heating of the fibre the polarization of the system remained stable over the measurement time (~30 minutes). If temperature fluctuations were induced in the fibre, the WDM configuration was found to be particularly stable in terms of timing and synchronization, but that the spatial multiplexing approach should also be viable with the addition of simple tracking electronics to the SPAD gate generator. The results confirm that InGaAs/InP SPADs currently appear to be the best detector choice for QKD systems operating over the distance range around and beyond 50 km.

Acknowledgments

This work was partly funded by the UK Engineering and Physical Sciences Research Council (No. GR/L81895), and the European Commission's Framework 5 EQUIS project (IST-1999-11594). The authors wish to thank Sara Pellegrini, of the Department of Physics at Heriot-Watt University, for her invaluable assistance in the construction of the 80 km spatial multiplexing system and in the stability measurements.

References

[1] Bennett, C. H., and Brassard, G., 1984, *Proceedings of the IEEE international conference on computers, systems and signal processing*, pp. 175–179.
[2] Bennett, C. H, Bessette, F., Brassard, G., Salvail, L., and Smolin J., 1992, *J.* Cryptol., **5,** 3.
[3] Marand, C., and Townsend, P. D., 1995, *Opt. Lett.*, **20,** 1695.
[4] Townsend, P. D., 1998, *Opt. Fibre Technol.*, **4,** 345.
[5] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., and Zbinden, H., 1998, *Electron. Lett.*, **34,** 2116.
[6] Hughes, R. J., Morgan, G. L., Peterson, C. G., 2000, *J. Modern Opt.*, **47,** 533.

[7] Bourennane, M., Gibson, F., Karlsson, A., Hening, A., Jonsson, P., Tsegaye, T., Ljunggren, D., and Sundberg, E., 1999, *Opt. Express*, **4,** 383.
[8] Lacaita, A., Zappa, F., Cova, S., and Lovati, P., 1996, *Appl. Opt.*, **35,** 2986.
[9] Hiskett, P. A., Buller, G. S., Loudon, A. Y., Smith, J. M., Gontijo, I., Walker, A. C., Townsend, P. D., and Robertson, M. J., 2000, *Appl. Opt.*, **39,** 6818.
[10] Ribordy, G., Gautier, J.-D., Zbinden, H., and Gisin, N., 1998, *Appl. Opt.*, **37,** 2272.
[11] Karlsson, A., Bourennane, M., Ribordy, G., Zbinden, H., Brendel, J., Rarity, J., and Tapster, P., 1999, *Circuits and Devices*, **15,** 34.
[12] Lutkenhaus, N., 2000, *Physical Rev.* A, **61,** 052304/1–10.
[13] Bennett, C. H., Brassard, G., Crepeau, C., and Maurer, U. M., 1995, *IEEE Trans. Inf. Theory*, **41,** 1915.
[14] Malitson, I. H., 1965, *J. Opt. Soc. Am.*, **55,** 1205.