New Journal of Physics
The open-access journal for physics

Long-distance quantum key distribution in optical fibre

P A Hiskett[1], D Rosenberg[1,4], C G Peterson[1], R J Hughes[1], S Nam[2], A E Lita[2], A J Miller[3] and J E Nordholt[1]

[1] Los Alamos National Laboratory, Los Alamos, NM 87545, USA
[2] National Institute of Standards and Technology, Boulder, CO 80305, USA
[3] Albion College, Albion, MI 49224, USA
E-mail: rosenberg@lanl.gov

New Journal of Physics **8** (2006) 193
Received 23 June 2006
Published 14 September 2006
Online at http://www.njp.org/
doi:10.1088/1367-2630/8/9/193

Abstract. Use of low-noise detectors can both increase the secret bit rate of long-distance quantum key distribution (QKD) and dramatically extend the length of a fibre optic link over which secure keys can be distributed. Previous work has demonstrated the use of ultra-low-noise transition-edge sensors (TESs) in a QKD system with transmission over 50 km. In this study, we demonstrate the potential of the TESs by successfully generating an error-corrected, privacy-amplified key over 148.7 km of dark optical fibre at a mean photon number $\mu = 0.1$, or 184.6 km of dark optical fibre at a mean photon number of 0.5. We have also exchanged secret keys over 67.5 km that is secure against powerful photon-number-splitting (PNS) attacks.

Many classical encryption schemes base their security on the perceived difficulty of efficiently performing certain computational tasks, such as the factoring of large numbers. Quantum key distribution (QKD), on the other hand, allows two users to create a shared, secret, random key for encrypting data, enabling communication that can be proven secure by the laws of physics [1]. Ideally, information is contained in the state of a single quantum, so an eavesdropper ('Eve') is unable to gain information without disturbing the system and revealing her actions. To implement QKD, it is necessary to have a source of single quanta, a method for encoding and decoding information on to and from these quanta, and a protocol for establishing a key. Photons are the obvious choice for sending information over large distances with little decoherence or loss. At present, there are no commercially available single photon sources, but a heavily attenuated, pulsed laser source provides a practical alternative. Photon statistics from such a laser source

[4] Author to whom any correspondence should be addressed.

PII: S1367-2630(06)27213-6

follow a Poisson distribution, where the probability of a multi-photon signal is approximately $\mu^2/2$ for mean photon number $\mu < 1$. The presence of these signals must be included in the secrecy analysis of the system, because an 'Eve' could gain information about multi-photon signals without being detected. Hypothetically, in the presence of channel loss an 'Eve' using a sophisticated (but presently unfeasible) photon-number-splitting (PNS) attack [2] could even gain complete knowledge of the key if the mean photon number, μ, exceeds a certain link-loss and therefore distance-dependent maximum value. Such upper limits on μ set a maximum QKD secret key transmission distance owing to the reduction in signal-to-noise with distance. In this paper, we show that maximum secret key transmission distances and rates can be dramatically extended by the use of ultra low-noise transition-edge sensor (TES) single-photon detectors in a novel optical fibre QKD system.

Long-distance fibre-based QKD systems such as the one described in this study usually use phase-encoding. In the 'prepare-and-measure' BB84 QKD protocol [3], the sender (Alice) encodes a random bit on to a photon using one of two randomly chosen conjugate bases, and sends it to the receiver (Bob). Bob then performs a measurement on the photon, randomly choosing one of the two possible bases. Their random basis choices are then shared over a public channel and only events where the same bases were used are retained, thereby creating a sifted key. Error correction [4] and privacy amplification [5] are applied to the sifted key to create a shorter, final secret key.

Fibre-based QKD systems usually operate at one of the telecommunications wavelengths where optical fibre has very low loss. Fibre has minimum loss of $\sim$0.2 dB km^{-1} at 1550 nm, but detector properties play a critical role in the performance of QKD systems and limit the length of a secure link. Most present-day optical fibre QKD systems use InGaAs/InP avalanche photo-diode (APD) detectors operated in Geiger mode. APDs have excellent timing resolution ($<$100 ps), but they suffer from low efficiencies ($\sim$20%), usually have large dark-count rates (tens of kilohertz) and require long dead times (several tens of microseconds) following photon detection[5], limiting maximum transmission distances to approximately 100 km. In contrast, the TES detectors used in this study [6] can be engineered to have much higher detection efficiency at the target wavelength [7], with much shorter dead-time, and they have no dark counts, although ambient blackbody radiation creates a background count rate that plays the same ultimate role in a QKD system. Despite present TES timing resolutions of order 100 ns, the high efficiency, low dark count rates, and shorter dead-time of TESs mean that their incorporation in a QKD system can enable key distribution over longer distances, at higher secret bit rates and with higher security. TESs have previously been integrated into a QKD system yielding secret key transmission over 50 km of low-dispersion fibre, and many of the associated experimental details have been discussed [8]. The TESs used in the present study had a detection efficiency of 65% at 1550 nm, a background count rate of 10 counts per second dominated by blackbody radiation, a timing resolution of 90 ns full-width-at-half-maximum, and a dead time of 4 μs.

A simplified schematic of the phase-encoding QKD system is shown in figure 1 and has been discussed in detail in [9]. The system operates at a clock rate of 1 MHz with a single 10 MHz rubidium clock providing synchronization for Alice and Bob[6]. A distributed feedback laser (DFB), operating at a wavelength of 1550 nm, is gain-switched to output pulses of width 100 ps. After passing through Alice's phase encoder, which time-multiplexes the signals on to

[5] See, for example, products by Princeton Lightwave and Sensors Unlimited.

[6] Single-clock synchronization is infeasible in a practical setting outside a laboratory, and a system is under development that uses independent clocks at Alice and Bob.

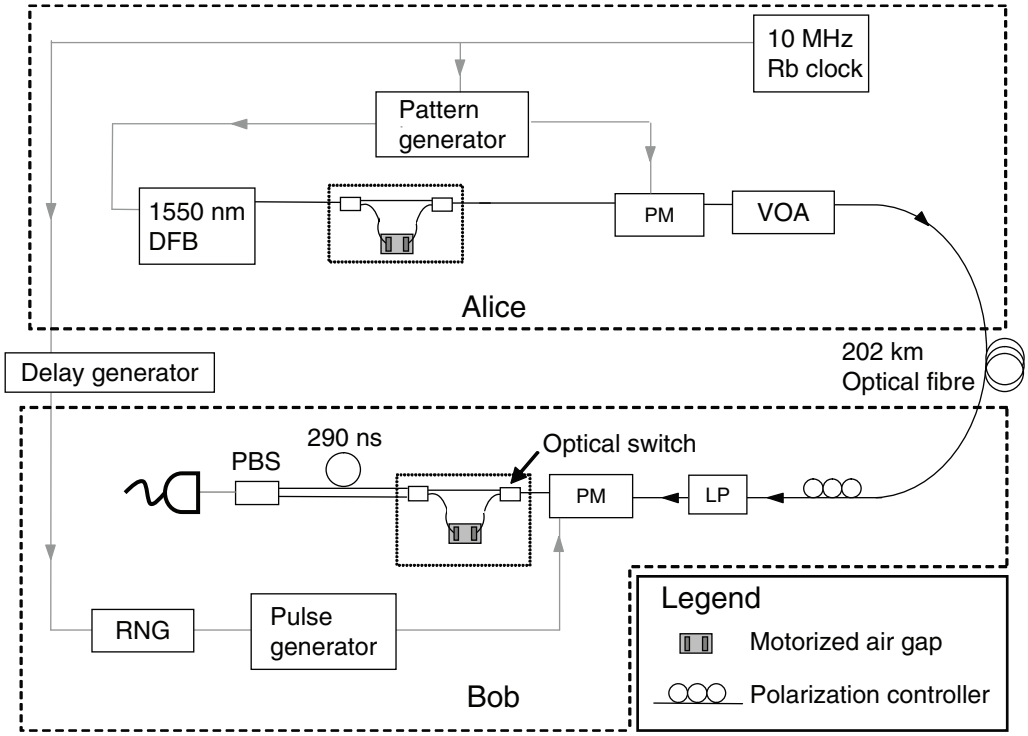

Figure 1. Simplified schematic of phase-coding QKD system. LP = linear polarizer; VOA = variable optical attenuator; PBS = polarizing beam splitter; DFB = distributed feedback laser; RNG = random number generator; PM = phase modulator.

one fibre, the optical signals are attenuated to the single-photon level and coupled into a spool of 202 km of single-mode fibre linked to Bob's phase decoder, which, together with Alice's encoder, comprises a single Mach–Zehnder interferometer. The mean photon number μ of the system is defined as twice the mean photon number of the part of the photon wavepacket that transits the long path of Alice's interferometer, at the point that it leaves her enclave. Alice and Bob encode information and choose measurement bases by applying phases to the photons appropriate for the BB84 protocol [10] using their respective fast electro-optic phase modulators, which are located external to their interferometers [11] for stability. Alice modulates only the phase of the part of the wavepacket that travels through the long path in her phase encoder, while Bob modulates the phase of the part that took her long path. BB84 data is communicated in Bob's detections of photons that take the interfering long-short or short-long paths. Typically in such phase-encoded systems, roughly one half of the transmitted signals yield no information, owing to photons that are either delayed or advanced by several ns relative to the data photons, corresponding to the long-short time difference between the paths in the encoder and decoder. For this system, the difference between the short and long paths is 10 ns. This would create a problem for detectors, such as the TES, that lack sufficient timing resolution to discriminate between the different arrival times. So, our system uses a novel switching technique at the input of Bob's interferometer to eliminate these amplitudes: the photon amplitude for Alice's short (long) path is switched on to Bob's long (short) path, respectively. This allows the TESs to be used in the system and doubles the implementation efficiency of a phase-encoded system. Due to

the insertion loss of the switch (2.3 dB), the key rate is not doubled but is instead approximately 17% higher than it would have been without the switch.

By inserting a 290 ns fibre delay into one of the output ports of Bob's phase decoder, and rotating the photon polarization in the delay path by 90°, both outputs are time-multiplexed on to a single optical fibre using a polarizing fibre splitter, allowing the receiver to operate with only one TES detector. A histogram of arrival times at the receiver relative to the 1 MHz clock signal displays two peaks, one of which contains events from '0' bits and the other which contains '1' bits after sifting [8]. The peaks are each 90 ns full-width-at-half-maximum and are spaced 290 ns apart. To define the sifted key bits, it is necessary to choose appropriate timing windows for the 0 and the 1 bits. Wide timing windows would encompass most of the counts in each channel, maximizing the sifted bit rate, but would also include many background counts, leading to a higher sifted bit error rate (BER). Narrower timing windows would contain fewer background counts, reducing the sifted BER, but would also reduce the sifted bit rate. We chose a width of the timing window to maximize the secret bit rate of the system; this optimal width depends on the rate of real counts compared to the rate of background counts [9]. In general, the optimal window width, which ranged from 30 to 170 ns, was narrower for longer distances or lower mean photon numbers.

Although the length of the fibre link is fixed at 202 km, shorter effective distances can be realized by redefining Alice's transmitter to contain some first portion of the 202 km optical fibre, which acts as an extra attenuator. The mean photon number μ of signals leaving Alice's enclave must then include the loss in this length of fibre. For example, consider transmissions with $\mu_{202} = 0.5$ at the input to the full 202 km of fibre. Redefining the system so that Alice includes the first 35.8 km of optical fibre, the transmission distance becomes 166.2 km, and we find that $\mu = 0.1$ at the output of the 'new' Alice, where we have used the measured attenuation of $\alpha = 0.195\,\mathrm{dB\,km^{-1}}$ for the optical fibre. In general, the relation between effective transmission distance, d_{eff}, and mean photon number μ is

$$d_{\mathrm{eff}} = d_0 + (10/\alpha)\log_{10}(\mu/\mu_{202}), \tag{1}$$

where $d_0 = 202$ km. Note that we have used this technique only to map the 202 km fibre link to *shorter* distances; mapping to longer distances would be nontrivial because of effects such as fibre dispersion. In figure 2 we show the sifted bit rate and sifted BER as a function of transmission distance for detection windows optimizing the secret bit rate. The sifted bit rate is consistent with the measured fibre loss, detector efficiency, and window widths, allowing for 7.98 dB loss within Bob's interferometer and optics. The dependence of the BER on window width (not shown) is consistent with the measured background count rate, and from the variation with window width, we infer that the portion of the BER that is due solely to interferometer visibility is 1.8%. This portion of the BER did not change significantly with mean photon number, demonstrating that we could successfully tune the interferometer even at very low mean photon numbers.

Figure 3 shows the secret bit rate as a function of effective transmission distance of the system, after error correction of the sifted key using the CASCADE algorithm [4], and 'BBBSS91' privacy amplification [12] as implemented in [13]. It is assumed that: the Alice–Bob quantum channel losses are random photon deletions with probability corresponding to the measured fibre attenuation; all sifted bits arising from multi-photon signals leaving Alice's enclave are known to Eve; all sifted bit errors are attributed to Eve having performed intercept-resend attacks in the Breidbart basis [12] on single-photon signals in the sifted key; and publicly communicated parity bits for error correction are known to Eve [14]. To facilitate comparison of

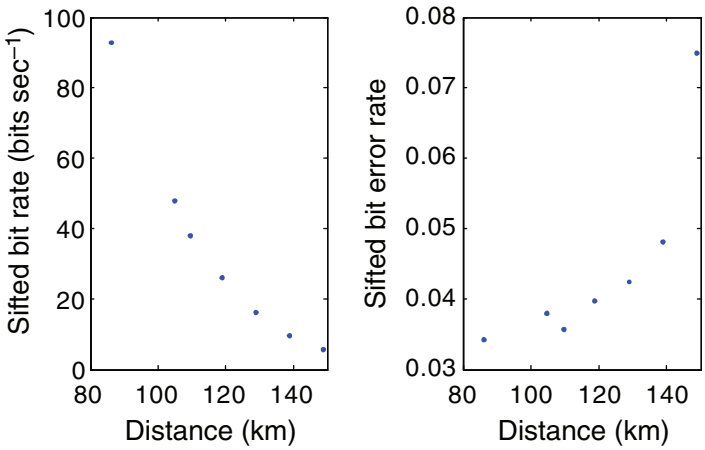

Figure 2. Sifted bit rate and BER as a function of distance at a mean photon number of $\mu = 0.1$ for optimal window widths. Distances shorter than 202 km were achieved by defining the first part of the fibre link to be within the transmitter's enclave, as discussed in the text.

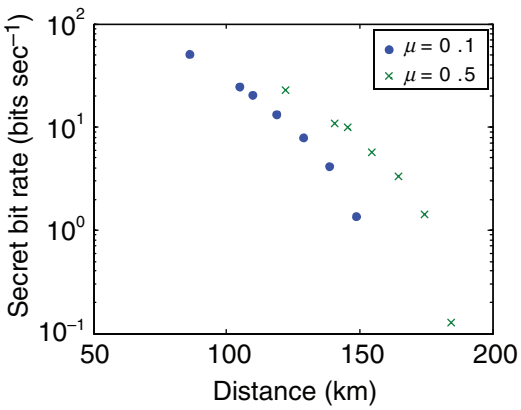

Figure 3. Secret bit rate as a function of transmission distance, analysed at $\mu = 0.1$ and 0.5.

our results with those of other groups, we have displayed our data at the canonical $\mu = 0.1$ value [12]. We report a new record maximum QKD transmission distance of 148.7 km at this photon number. From a total of 5644 sifted bits, we produced 1307 secret bits at a rate of 1.36 secret bits per second (b.p.s) at this distance. However, the choice of $\mu = 0.1$ is arbitrary. Operation at higher μ yields a higher sifted bit rate and lower sifted BER, but requires more privacy amplification because of the increased likelihood of multi-photon events: for each transmission distance there is an optimal value of μ for which the secret bit rate is maximized. In general, it is unlikely for a given system that this optimal value is 0.1. If we use equation (1) to map the data for $\mu = 0.1$ to a higher value of μ, the effective transmission distance becomes longer, shifting the $\mu = 0.1$ curve in figure 3 to the right. However, the increased privacy amplification necessary at higher μ also shifts the curve down, until the secret bit rate for the data point furthest to the right crosses zero. At this point, we have reached the maximum transmission distance of our system with BBBSS91 privacy amplification. For our data, the cutoff occurs just over $\mu = 0.5$ and yields

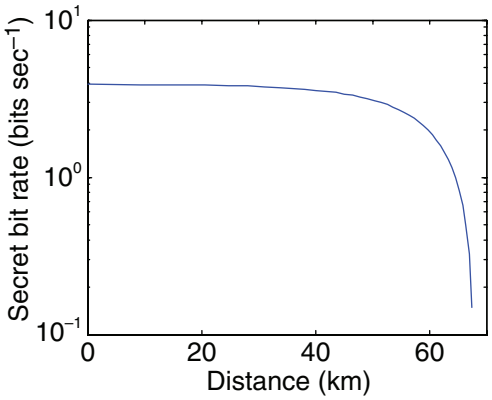

Figure 4. Secret bit rate as a function of distance for data secure against general PNS attacks. The secret bits were generated from 13 350 sifted bits with a BER of 5.3%.

a maximum transmission distance of 184.6 km. A key created at this mean photon number over this distance is susceptible to an unambiguous state discrimination attack [15], but security in this parameter regime can be ensured with the use of a decoy state protocol to protect against this and stronger attacks.

In the adversarial context of QKD the random-deletion channel assumption of BBBSS91 privacy amplification cannot be rigorously justified with the simple BB84 protocol. For instance, in a PNS attack Eve could hypothetically block all the single photon signals, remove one photon from each multi-photon signal and store it in a quantum memory, and send the remaining photons from each multi-photon signal over a loss-free channel to keep Bob's signal detection rate unchanged. Once the bases are announced, Eve could measure her stored photons and gain complete knowledge of the key. Within the simple BB84 protocol, protection against PNS attacks requires operation at mean photon numbers low enough to ensure that at least some of the sifted bits arise from single-photon signals. As with the previous data, we can transmit over the 202 km link and then redefine μ at shorter transmission distances. As the distance gets shorter, the mean photon number becomes smaller until it is eventually low enough so that PNS-secure transmission is possible. Performing privacy amplification against general [16] PNS attacks and making the conservative assumption that all of Bob's losses are accessible to Eve, this occurs at 67.5 km, at which point $\mu = 0.0041$. Therefore, we are able to create PNS-secure key at distances shorter than or equal to 67.5 km, as shown in figure 4.

Using ultra-low-noise, high-efficiency TES detectors in a novel optical fibre QKD system at 1550 nm, we have set several new secret key transmission distance records. To the best of our knowledge, at the time this paper was written the distance record for secret key creation in a system with $\mu = 0.1$ was 122 km[7] [18]. We have now increased this record distance by 22% to 148.7 km. The previous record distance for key creation using weak laser pulse QKD with the simple BB84 protocol secure against individual PNS attacks was 50.6 km [19]. We have increased this record distance by more than 30%, and also surpassed by several kilometres the maximum

[7] Another group has achieved single-photon interference with greater than 80% visibility over a link of 150 km; but their system, which transmitted at $\mu = 0.2$ and did not include phase modulators, was not used to create secret key [17].

PNS-secure transmission distance inferred in a recent 'decoy state' protocol implementation with conventional detectors [20]. Our demonstration of secret key production at 184.6 km at $\mu = 0.5$ under the assumption of a random deletion channel is a new, absolute distance record for QKD. This result indicates that PNS-secure QKD could be extended well into the greater than 100 km transmission distance regime using TES detectors with a decoy state protocol: the decoy states would provide rigorous justification for the channel properties, without additional assumptions. We observe that our new methodology of using a detection time-window selected to maximize the secret bit rate is likely to be of great value in optimizing the performance of other QKD systems. Finally, we note that significant reductions in TES timing jitter and dead-time are feasible with fairly straightforward improvements in the detector electronics, potentially opening the door to higher secret bit rates over the long transmission distances demonstrated here.

Acknowledgments

We thank Alan Migdall for the loan of an optical switch and Joe Dempsey of Corning Inc. for the loan of the 202 km of SMF 28e® optical fibre. We note that our measurement of 0.195 dB km^{-1} is slightly higher than is expected for SMF 28e® and we attribute this to splices in our system. Jim Harrington is thanked for helpful discussions. DR thanks the DCI postdoctoral program. SN acknowledges the support of the DARPA QuIST program and NIST Quantum Initiative. This work was supported in part by DTO.

References

[1] Quantum cryptography roadmap, online at http://qist.lanl.gov
[2] Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* p 175
[4] Brassard G and Salvail L 1994 *Lecture Notes Comput. Sci.* **765** 410
[5] Bennett C H, Brassard G, Crepeau C and Maurer U M 1995 *IEEE Trans. Inf. Theory* **41** 1915
[6] Cabrera B, Clarke R M, Colling P, Miller A J, Nam S and Romani R W 1998 *Appl. Phys. Lett.* **73** 735
[7] Rosenberg D, Lita A E, Miller A J and Nam S 2005 *Phys. Rev.* A **71** 061803 (R)
[8] Rosenberg D, Nam S, Hiskett P A, Peterson C G, Hughes R J, Nordholt J E, Lita A E and Miller A J 2006 *Appl. Phys. Lett.* **88** 021108
[9] Hiskett P A, Peterson C G, Hughes R J, Rosenberg D, Nam S, Lita A E and Nordholt J E 2006 *Los Alamos report* LA-UR-06-3211
[10] Hughes R J *et al* 2000 *J. Mod. Opt.* **47** 533
[11] Hughes R J *et al* 2005 *Proc. SPIE* **5893** 1
[12] Bennett C H *et al* 1992 *J. Cryptol.* **5** 3
[13] Hughes R J *et al* 2002 *New J. Phys.* **4** 43.1
[14] Cachin C and Maurer U M 1997 *J. Cryptol.* **10** 97
[15] Dusek M, Jahma M and Lutkenhaus N 2000 *Phys. Rev.* A **62** 022306
[16] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[17] Kimura T, Nambu Y, Hatanaka T, Tomita A, Kosaka H and Nakamura K 2004 *Japan. J. Appl. Phys.* **43** L1217
[18] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[19] Gobby C, Yuan Z L and Shields A J 2004 *Electron. Lett.* **40** 1603
[20] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Preprint* quant-ph/0601168