Title	Robust gigahertz fiber quantum key distribution
Authors	Clarke, Patrick J.;Collins, Robert J.;Hiskett, Philip A.;Townsend, Paul D.;Buller, Gerald S.
Publication date	2011
Original Citation	Clarke, P. J., Collins, R. J., Hiskett, P. A., Townsend, P. D. and Buller, G. S. (2011) 'Robust gigahertz fiber quantum key distribution', Applied Physics Letters, 98(13), pp. 131103. doi: 10.1063/1.3571561
Type of publication	Article (peer-reviewed)
Link to publisher's version	http://aip.scitation.org/doi/abs/10.1063/1.3571561 - 10.1063/1.3571561
Rights	© 2011 American Institute of Physics.This article may be downloaded for personal use only. Any other use requires prior permission of the author and AIP Publishing. The following article appeared in Clarke, P. J., Collins, R. J., Hiskett, P. A., Townsend, P. D. and Buller, G. S. (2011) 'Robust gigahertz fiber quantum key distribution', Applied Physics Letters, 98(13), pp. 131103 and may be found at http://aip.scitation.org/doi/abs/10.1063/1.3571561
Download date	2023-03-29 17:31:15
Item downloaded from	http://hdl.handle.net/10468/4323

Robust gigahertz fiber quantum key distribution

Patrick J. Clarke' , Robert J. Collins' , Philip A. Hiskett, Paul D. Townsend, and Gerald S. Buller'

Robust gigahertz fiber quantum key distribution

Patrick J. Clarke,[1,a] Robert J. Collins,[1,b] Philip A. Hiskett,[1] Paul D. Townsend,[2] and Gerald S. Buller[1,c]

[1]*School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

[2]*Department of Physics and Tyndall National Institute, Photonics Systems Group, University College Cork, Cork, Ireland*

We present recent results on an innovative fiber based short wavelength gigahertz clock rate quantum key distribution system operating over a standard telecommunications optical fiber quantum channel. This system is designed to be robust against environmentally induced changes in the polarization evolution of the photons in the optical fiber quantum channel and against path-length drift in the interferometers which could otherwise compromise system performance. Experimental results are presented for error rate, net bit rate and stability for different silicon single-photon avalanche diode detector types. © *2011 American Institute of Physics.* [doi:10.1063/1.3571561]

Quantum key distribution (QKD) has been the subject of a great deal of research over the last two and a half decades,[1] during which the community has continued to develop faster, lower error rate QKD systems. Many of these systems operate at wavelengths (λ) around 1.3 and 1.55 μm in the telecommunications optical fiber low loss windows in order to maximize system reach. However, the commonly available single-photon detectors for these λ can suffer from afterpulsing effects and increased timing jitter which necessitates operation at low clock frequencies and/or gated operation.[2] The comparatively more mature silicon based single-photon avalanche diodes (Si-SPADs) available for use in the λ range ~400 nm to ~1 μm offer lower timing jitter, reduced afterpulsing and can be operated in free-running mode.[2,3] The fiber attenuation is greater at these operational λ, with the wavelength of 850 nm selected as a compromise between reasonable attenuation (~2.2 dB km^{-1}) and detector efficiency. Operation at clock rates of up to 3 GHz has been demonstrated using thick junction Si-SPAD detectors in a QKD system at ~850 nm wavelength.[4] However, thick junction Si-SPADs can exhibit full-width at half maximum (FWHM) timing jitter of ~400 ps which can, at high clock frequencies, lead to intersymbol interference and significantly increase the quantum bit error rate (QBER) of the QKD system.[5] Thin-junction Si-SPADs generally exhibit lower timing jitter but also exhibit reduced detection efficiencies and long tails in the timing response.[6] A typical commercial thick junction Si-SPAD can have detection efficiencies of the order of 40% for λ~850 nm compared to approximately 10% for a thin junction Si-SPAD.[2]

In this letter, we present a 1 GHz clock rate QKD system operating at λ~850 nm in fiber which is designed to be robust against environmentally induced changes in polarization evolution in the quantum channel and changes in the path-lengths of the interferometers. Short wavelengths offer the advantage that they are widely spectrally separated from the classical data communications at λ~1.3 μm and ~1.55 μm present in the fibers. Hence, the quantum channel

avoids the spectrally wide spontaneous Raman scattering background generated by the high power classical data channels, which can considerably increase the QBER in the QKD system.[7] The higher fiber losses mean that transmission distances are limited to those consistent with the ~10 km distances typically employed in optical access applications.[4] We compare the operation of the system with several Si-SPAD detector geometries and examine the effect of detector performance on the overall QKD performance.

The system is shown schematically in Fig. 1, and uses the four-state BB84 protocol,[1] with the encoding and decoding provided by phase changes in Mach–Zehnder interferometers. We have added a compact Lyot-type depolarizer after the output fiber from Alice.[8] The 45° splice at the input of the depolarizer equally excites two orthogonal polarization modes in the polarization maintaining (PM) fiber which are equally split at the polarization beamsplitter. One output arm is delayed with respect to the other, with the delay being longer than the coherence time of the source (33 ps) but shorter than the laser pulse duration (53 ps) so that when
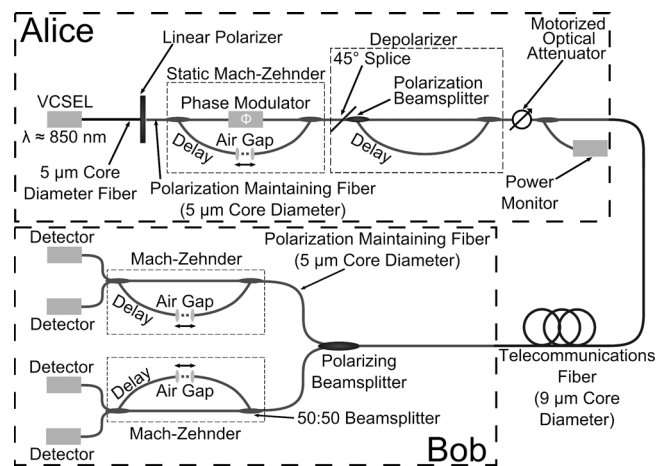

FIG. 1. A schematic of the robust QKD system. The air gap in the transmitter is fixed for the duration of a measurement while those in receiver are adjusted under computer control to maintain the maximum fringe visibility in each interferometer. Alice and Bob's interferometers are constructed from PM fiber to ensure good fringe visibility.

a)Electronic mail: pjc14@hw.ac.uk.
b)Electronic mail: r.j.collins@hw.ac.uk.
c)Electronic mail: g.s.buller@hw.ac.uk.

recombined the two beams are incoherent and cannot be time resolved with the detectors used. Depolarized light is achieved when the two orthogonal polarizations are combined with equal intensities at the final beam-combiners. The path delay introduced by the depolarizer does not change or depend upon the information content of the key, so an eavesdropper capable of resolving this will gain no extra information. The depolarizers randomizes the polarization of the photons entering the standard telecommunications fiber (SMF-28e) quantum channel, thus preventing the environmentally induced changes in fiber birefringence from altering the polarization state. To ensure high fringe visibility in Bob's interferometers it is necessary to have the same polarization in each arm when incident on the beam-combiners. However, interferometers based on standard (non-PM) fiber and components typically exhibit sufficient birefringence that the achieved fringe visibility varies significantly with input polarization state. This problem is avoided here by depolarizing the quantum channel and constructing Alice and Bob's interferometers from PM fiber, which fixes the polarization states in each arm. A polarizing beamsplitter at Bob's input then randomly routes the depolarized photons into one of the two fixed interferometers, one for each of the two basis sets, linearly polarizing them as it does so. This allows us to achieve visibilities of 98%, which are stable with time. Alternative schemes would either require the additional complexity and cost of active polarization control or the use of a 50:50 beamsplitter with a polarizer prior to each of the interferometers, leading to a 50% signal loss.

Two interferometers are utilized at Bob in place of the combination of a single interferometer and an active phase modulator to avoid any thermal instability from the active component. The QBER is monitored in the control computer, and automatic adjustments are made of the air-gaps via a piezoelectric adjuster. In this way, any small drift in path-length between Alice's single interferometer and the two interferometers in Bob is automatically compensated. Alice monitors the transmitted photon flux and adjusts the motorized optical attenuator to maintain a constant mean photon number.

The interferometers used by both Alice and Bob are constructed from 5 μm core PM fiber which is single mode at $\lambda \sim 850$. The 9 μm core diameter SMF-28e fiber is multimodal for $\lambda \sim 850$ nm and mode control techniques were used to suppress the higher order modes.[5] Concentrically splicing short (<1 m) lengths of 5 μm fiber onto the input and output of the standard telecommunications optical fiber quantum channel ensures that $>99\%$ of the photons are launched into the fundamental LP_{01} mode.[9]

In the system presented here, the QBER can be expressed as containing contributions from the visibility of the interferometers, errors in the phase encoding, the dark counts of the detector and the timing jitter of the complete system

$$QBER_{total} = QBER_{visibility} + QBER_{phase} + QBER_{dark}$$
$$+ QBER_{jitter}. \quad (1)$$

At short distances, intersymbol interference will typically be the highest contribution to the total. As the transmission distance and hence the channel loss increases, the photon detection rate will eventually become sufficiently low that the dark count rate (DCR) of the detectors begins to dominate and the QBER increases. The contributions from visibility
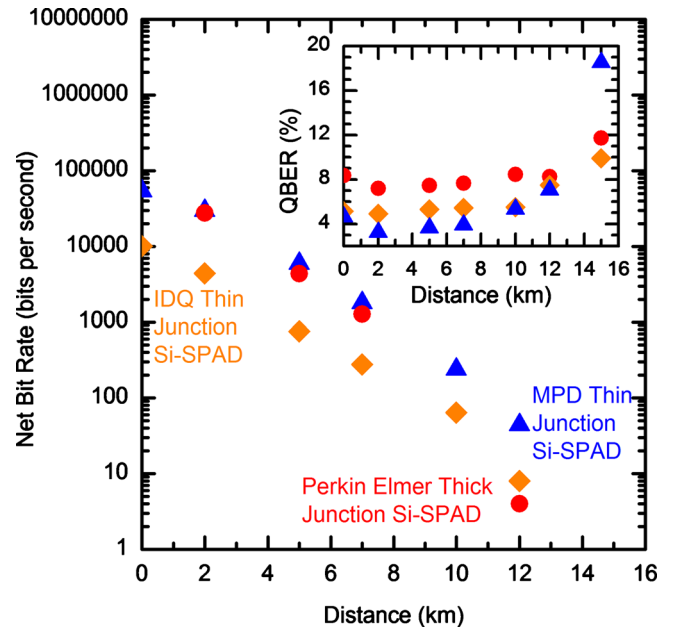

FIG. 2. (Color online) NBR (rate of final key) against quantum channel transmission distance for three different detectors. The inset shows the minimum QBER against quantum channel transmission distance for the detectors.

and phase encoding errors also remain constant but are typically lower than that induced by dark counts in this system. An estimation of the combined QBER contribution from visibility and phase errors in this system is 1.8%.

We compared the system performance using three different types of Si-SPAD: a 100 μm active area diameter PerkinElmer SPCM AQR 12 thick junction Si-SPAD, a 20 μm active area diameter thin junction Micro Photo Devices (MPD) PDF CCTC Si-SPAD and a 50 μm active area diameter IDQ id100-MMF50 thin junction complementary metal-oxide semiconductor Si-SPAD. All three detectors were peltier cooled to an operating temperature in the range $\sim 230–260$ K. The inset in Fig. 2 shows the lowest QBER as a function of distance using the different single-photon detectors. The characteristic shape of the curve is primarily determined by the timing jitter, DCR and the detection efficiency (DE) of the detector. The thick junction PerkinElmer Si-SPAD exhibits a baseline QBER of about 7.2% which is higher than those observed when using thin junction Si-SPADs. The instrumental response for the thick-junction Si-SPAD has a FWHM of 432 ps in comparison to ~ 67 ps for both thin junction Si-SPADs at a clock rate of 1 GHz. Consequentially there is a higher possibility of photons being detected in an incorrect window thereby increasing the baseline QBER, as shown in Fig. 2. However, if the FHWM jitter is similar, then the long tail in the timing response—caused by the relatively slow diffusion of carriers generated from deeply absorbed photons—will significantly increase the QBER. The higher baseline QBER obtained using the IDQ SPAD in comparison to the MPD, which both have a similar FWHM, is partially due to the longer tail and partially due to the decreased DE of 1.6% as opposed to 8.4%.

The detector parameters which determine the distance at which the QBER begins to increase dramatically are the DCR and the DE of the detector, as illustrated by the comparisons in Fig. 2. Higher DE and lower DCR moves this point to longer distances by increasing the number of photo-

generated events detected relative to the unwanted noise contributions from the DCR and background light.

Following basis set reconciliation the detected photon events are temporally filtered to reduce the effect of dark counts using a gate of duration 100 ps centered around the most probable detection time and correction of errors in the key shared between Alice and Bob is performed.[10] The system presented in this paper uses weak coherent pulses to simulate ideal single photon states. Therefore a certain percentage of pulses (~5% in this case) contain multiple photons. In theorem 6 of their 2004 paper Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) (Ref. [11]) indicate a security boundary for a BB84 QKD system. Our postprocessing software applies a technique based on the principles of GLLP security analysis to the generated key. We approximate the tagged multiphoton term of GLLP as $\mu^2/2$ and do not take into account channel loss. This means that although we maintained a constant mean photon number per pulse (μ) in our experiments our analysis indicates how the system would respond if decoy states[12] were applied. The main Fig. 2 shows the highest net bit rates (NBR) achieved with this system. Although the thick junction Si-SPAD has the highest baseline QBER due to the FWHM timing jitter, the high DE of ~42% meant that, after postprocessing, the final NBR was the second highest. The lowest QBER and highest NBR at distances less than 12 km was exhibited by a thin junction detector from MPD despite this device only having a DE of 8.4%. At distances over 12 km the DCR of 200 counts s^{-1} of the MPD Si-SPAD leads to a faster increase in QBER than observed for the IDQ Si-SPAD which had a DCR of 15 counts s^{-1}.

To demonstrate the stability of the system to environmental fluctuations data was continuously acquired over the course of 24 h with a 2 km quantum channel using the MPD Si-SPAD. The custom control software monitored the QBER and once this reached a threshold value key generation was temporarily halted and the interferometers at Bob were automatically retuned using multiphoton classical pulses to a high visibility before μ was returned to 0.1 and key exchange resumed. Figure 3 shows the fluctuations in the QBER and NBRs over the course of the measurement. During this 24 h acquisition period, no operator intervention was used, and the QBER was less than the threshold for 89% of the time with an average QBER of 6.4% and an average NBR of 12000 bits per second. The residual degree of polarization with the depolarizer was ~9%. We finally verified the function of our system by removing the depolarizer which increased the standard deviation in the raw bit rate measured at one of Bob's interferometers by a factor of 11. Following this, we further replaced the polarization beamsplitter with a fiber 50:50 beamsplitter which lead to a decreased visibility of 67%, equivalent to a QBER contribution of 16.5%.

This result demonstrates that the system is capable of fully autonomous operation for extended periods with comparatively short time spent retuning. The addition of a depolarizer to Alice negates polarization evolution of the transmitted photons which could compromise system performance. Active feedback tuning of the interferometers rapidly compensates for path length drift, reducing the QBER, and constant monitoring of mean photon number aids security. The visibility of this system ensures a low contri-
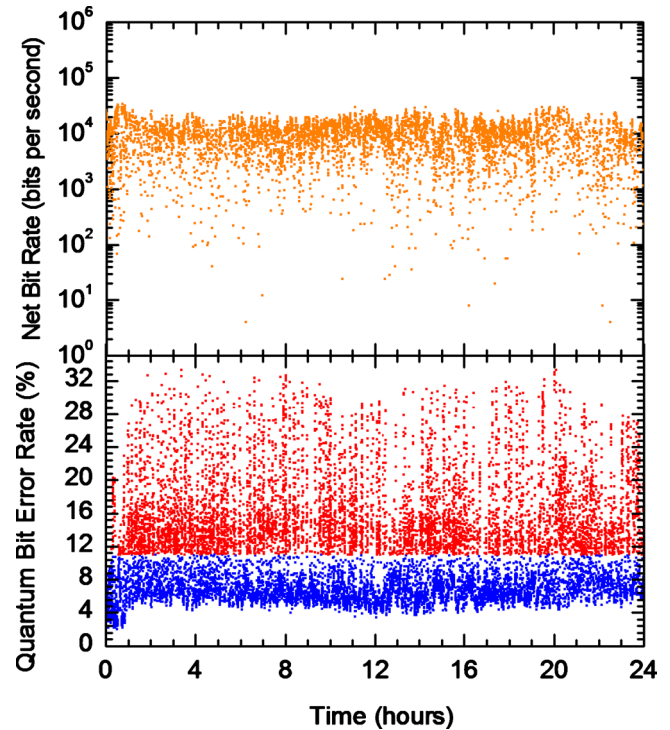

FIG. 3. (Color online) QBER (lower graph) and NBR (upper graph) against time for a 24 h fully automated operation of the QKD system. When the QBER exceeded a threshold of 11% automatic tuning was initiated. QBER points below 11% denote operation with key exchange while those above 11% denote tuning.

bution to the error rate from nonideal passive components. We demonstrated that the greatest single contribution to the overall QBER is from the detectors. Further analysis of the detector parameters and different detector geometries will permit a better understanding of more specific design routes for detectors used in QKD.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] G. S. Buller and R. J. Collins, Meas. Sci. Technol. **21**, 012002 (2010).
[3] E. Meyer-Scott, H. Hübel, A. Fedrizzi, C. Erven, G. Weihs, and T. Jennewein, Appl. Phys. Lett. **97**, 031117 (2010).
[4] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, IEEE J. Quantum Electron. **43**, 130 (2007).
[5] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, Opt. Express **13**, 3015 (2005).
[6] M. Ghioni, A. Gulinatti, I. Rech, F. Zappa, and S. Cova, IEEE J. Sel. Top. Quantum Electron. **13**, 852 (2007).
[7] I. Choi, R. J. Young, and P. D. Townsend, Opt. Express **18**, 9600 (2010).
[8] L. Li, J. Cardenas, J. Jiang, and G. P. Nordin, Opt. Eng. (Bellingham) **45**, 055602 (2006).
[9] P. D. Townsend, IEEE Photonics Technol. Lett. **10**, 1048 (1998).
[10] G. Brassard and L. Salvail, *EUROCRYPT '93: Workshop on The Theory and Application of cryptographic Techniques on Advances in Cryptology* (Springer, Berlin, 1994).
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).