Analysis of detector performance in a gigahertz clock rate quantum key distribution system

New Journal of Physics

The open-access journal for physics

Analysis of detector performance in a gigahertz clock rate quantum key distribution system

Patrick J Clarke[1], Robert J Collins[1], Philip A Hiskett[1,5], María-José García-Martínez[1,6], Nils J Krichel[1], Aongus McCarthy[1], Michael G Tanner[1], John A O'Connor[1], Chandra M Natarajan[1], Shigehito Miki[2], Masahide Sasaki[2], Zhen Wang[2], Mikio Fujiwara[2], Ivan Rech[3], Massimo Ghioni[3], Angelo Gulinatti[3], Robert H Hadfield[1], Paul D Townsend[4] and Gerald S Buller[1,7]

[1] Scottish Universities Physics Alliance and School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK

[2] National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan

[3] Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milano, Italy

[4] Tyndall National Institute and Department of Physics,
University College Cork, Cork, Ireland

E-mail: G.S.Buller@hw.ac.uk

New Journal of Physics **13** (2011) 075008 (23pp)
Received 28 March 2011
Published 22 July 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/7/075008

Abstract. We present a detailed analysis of a gigahertz clock rate environmentally robust phase-encoded quantum key distribution (QKD) system utilizing several different single-photon detectors, including the first implementation of an experimental resonant cavity thin-junction silicon single-photon avalanche diode. The system operates at a wavelength of 850 nm using standard telecommunications optical fibre. A general-purpose theoretical model for the performance of QKD systems is presented with reference to these experimental results before predictions are made about realistic detector developments in this system. We discuss, with reference to the theoretical model, how detector operating parameters can be further optimized to maximize key exchange rates.

[5] Present address: SELEX Galileo, Ferry Road, Edinburgh, UK.

[6] Present address: Consejo Superior de Investigaciones Científicas, Madrid, Spain.

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

Contents

1. Introduction

Quantum key distribution (QKD) is currently the only means by which Alice, the authorized sender, can distribute a cryptographic key to Bob, the authorized receiver, with verifiable security [1]. The first experimental demonstration of QKD was made in 1992 [2], and experimental research since then has mainly been focused on increasing the transmission distance, the clock rate [3] and/or the key exchange rate [4]. To date, clock rates of up to 10 GHz over channel losses of 50 dB [3] and secure key exchange rates of up to 1.002 Mbit s^{-1} have been achieved in laboratory conditions [4]. Much of this research has taken place on optical fibre-based systems operating at wavelengths around 1310 and 1550 nm, where the attenuation of standard telecommunications optical fibre is low, i.e. approximately 0.2–0.3 dB km^{-1}. This reduced fibre attenuation leads to the potential advantage of increased transmission length when compared with those systems operating at shorter wavelengths. However, the semiconductor detectors used at these wavelengths typically suffer from comparatively high dark count rates and after-pulsing probability [5], which can serve to limit the maximum achievable clock rate. At the shorter wavelengths, e.g. below 1000 nm, there is a wider availability of different single-photon detector types than at the telecommunications windows at ∼1310 and ∼1550 nm. In this paper, we present an experimental QKD testbed operating at a wavelength of 850 nm, which has permitted the convenient use of five different single-photon detector types, allowing an extensive comparison with the model presented in this paper. The relatively mature silicon single-photon avalanche diode (Si-SPAD) detectors generally exhibit considerably less of these deleterious afterpulsing effects, but operate efficiently only at shorter wavelengths (typically up to ∼1000 nm), which experience higher attenuation in the standard telecommunications optical fibre quantum channel. We have selected a wavelength of 850 nm as offering a suitable balance between channel loss (∼2.2 dB km^{-1}) and the detection efficiency of commercially available thick-junction Si-SPADs [6].

The implementation of the quantum channel at a wavelength of 850 nm has the advantage that it is widely separated spectrally from the data communications channels operating at wavelengths of ∼1310 and ∼1550 nm present in installed telecommunications optical fibre [7, 8]. While the spectrally narrow data channels can be routinely filtered from the quantum channel, the use of much shorter wavelengths avoids the broad spectrum of the Raman scattering background from the co-propagating data channels. This Raman background—typically hundreds of nm broad—can considerably increase the quantum bit error rate (QBER) in QKD systems with quantum channels operating near the data communications wavelengths [9]. The use of photons with a wavelength of 850 nm in the quantum channel gives the realistic possibility of co-propagation with other data transmission channels in the same fibre. These other data transmission channels will be a source of broadband Raman scattering at a level sufficient to cause false counts in the quantum channel receiver, consequently introducing a significant source of error in the quantum key exchange process [9]. The co-propagation of data and quantum channels is an essential consideration for use in installed metropolitan or access networks. In addition, short wavelengths also offer compatibility with single-photon sources [5] based on impurities in diamond or semiconductor quantum dots embedded in microcavities [10], although longer-wavelength demonstrations have also been made [11].

There are many different single-photon detector technologies available for use at a wavelength of 850 nm, some of which will be summarized in section 2. The characteristics of different single-photon detectors have a significant bearing on the overall system performance of the QKD system that employs them. To understand the combination of detector parameters that are desirable for efficient QKD, it is necessary to develop a comprehensive theoretical model of an experimental system. As described in section 3, we have developed a robust phase-basis set encoded QKD system operating at short wavelengths in standard telecommunications optical fibre [12] using the BB84 protocol. This system is capable of autonomous operation for long durations and representative results for a period of 24 h will be presented.

In section 4, we present a general purpose mathematical model that, although explained in terms of this system, is adaptable to any generic QKD system including those operating at different wavelengths, in free-space transmission and/or different QKD protocols. In section 5, the model is applied to our experimental system with different detectors, and in section 6, predictions about future QKD system performance are made based on realistic detector developments.

2. Single-photon detectors for use at a wavelength of 850 nm

A number of previous demonstrations of QKD at a wavelength of 850 nm have used thick-junction Si-SPADs as the detectors [6, 13]. While offering good detection efficiencies of $\sim$40% at this wavelength, these detectors also exhibit relatively long full-width at half-maximum (FWHM) timing jitters of $\sim$400 ps. Timing jitters of this duration can lead to intersymbol interference at clock rates [14] in excess of $\sim$1–2 GHz (depending on the exact optical system design) as the timing jitter exceeds the clock period, resulting in photon events being recorded in successive bit periods. Thin or shallow junction Si-SPADs offer shorter duration FWHM timing jitters of $\sim$70 ps, but can exhibit long tails in their timing profile caused by relatively slow diffusion of photo-generated carriers into the device multiplication region [15]. These diffusion tails can be characterized by the full-width at 10th-maximum (FW10%M) and full-width at 100th-maximum (FW1%M) timing jitters, as can be observed in the timing histograms shown in figure 1 and reported numerically in table 1. These thin-junction detectors generally exhibit reduced detection efficiencies of $<$10% at this wavelength.

The detection efficiency of a thin-junction Si-SPAD may be enhanced without compromising temporal response and dark count rate (DCR) by the use of a resonant cavity to increase the effective interaction length for absorption of incident photons [16]. The lower mirror of the resonant cavity is formed by the two layers of buried SiO_2 in the silicon substrate,

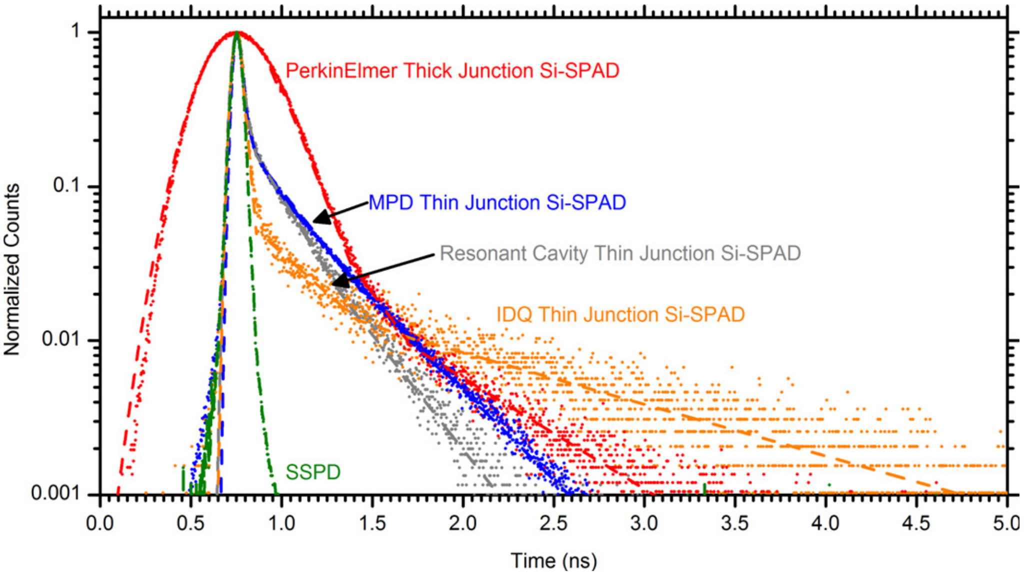

Figure 1. Normalized instrument responses for the specific detectors when used in the QKD system. The dashed lines represent a piecewise exponential fit used in the theoretical model.

Table 1. Characteristic parameters of the specific detectors when used at a wavelength of 850 nm in the QKD system.

Type	Detector	DCR (s^{-1})	Detection efficiency (%)	FWHM (ps)	FW10%M (ps)	FW1%M (ps)
Thick-junction Si-SPAD	PerkinElmer	198	42	432	837	1473
Thin-junction Si-SPAD	MPD	200	8.4	71	276	898
	IDQ	15	1.6	63	193	1245
	Resonant cavity	21	18	74	271	913
NbN superconducting nanowire	SSPD	10	10	62	120	196

and the upper mirror is formed by the silicon/air interface. The upper, low-doped p-epilayer contains the active n^+p-junction of the detector with an active area of 20 μm diameter. The complete epilayer structure had a thickness of 5 μm. In the results shown in this paper, this detector was operated at 260 K. The instrument response of such a detector can be seen in figure 1, where it may be observed that it is comparable with that of a similarly structured thin-junction Si-SPAD from Micro Photon Devices (MPD), which was grown on an all-silicon substrate and did not incorporate a resonant cavity. The resonant-cavity-enhanced detectors have recently been successfully employed in a low-light-level time-of-flight depth profiler operating at a similar wavelength [17] and their performance has been comparatively assessed in this context [18]. This paper presents the first application of such detectors to QKD.

In recent years, there has been a great deal of interest in the use of nanowire superconducting single-photon detectors (SSPD) [3, 19]. These detectors are based around a thin, narrow strip of a superconducting material, such as niobium nitride (NbN), that is biased at close to the critical current when cooled to a temperature of 3 K, a temperature that is below the superconducting transition temperature. An incident photon creates a resistive hotspot as the current density in parts of the nanowire exceeds the critical level, which leads to a readily detectable current pulse. The thin-junction Si-SPADs and the SSPD exhibit comparable FWHM timing jitters. However, in contrast, the SSPDs have an approximately Gaussian temporal response, as can be seen in figure 1. An SSPD may be operated at a number of different bias currents—as the bias current is increased, the detection efficiency increases but the DCR also increases. In the experiments described in this paper, the SSPDs have a detection efficiency of $\sim$10% for light at a wavelength of 850 nm when used with a DCR level of $\sim$10 counts s^{-1}. SSPDs have previously been demonstrated at GHz clock rates in various QKD demonstrations, including a polarization basis set, short-wavelength QKD system, and at a wavelength of 1550 nm [3], and full field-tests on installed optical fibre [20].

The QKD system presented in the following section has been operated using a 180 μm active area diameter PerkinElmer SPCM AQR 12 thick-junction Si-SPAD [21], a 20 μm active area diameter thin-junction MPD PDM CCTC Si-SPAD [22], a 50 μm active area diameter IDQ id100-MMF50 thin-junction CMOS Si-SPAD [23], an experimental 20 μm diameter active area resonant cavity thin-junction Si-SPAD [16] and an NbN nanowire meander line SSPD with a meander area of 20 μm$\times$20 μm and a fill factor of 50% [24]. The semiconductor detectors were peltier-cooled to an operating temperature in the range of $\sim$230–260 K, whereas the SSPD was operated at a temperature of 3 K in a closed-cycle refrigerator [25].

3. Experimental system

The robust experimental system is shown in figure 2. This setup is based on an asymmetric double Mach–Zehnder design. The delay in Alice establishes a phase reference for the quantum state set by the phase modulator in the short arm, while the equal delay in Bob allows for interferometric recombination of photons that have taken different paths at the final beamsplitter. Asymmetric double Mach–Zehnder designs commonly employ an active phase modulator at Bob to perform a basis set selection. However, this active component can induce thermal instability in the system and affect long-running operation. Instead, our robust variant employs two unbalanced Mach–Zehnder interferometers at Bob, one for each of the two basis sets [1], in order to improve thermal stability and facilitate long-term, continuous usage. Additionally, a depolarizer is employed at Alice to prevent environmentally induced changes in the birefringence of the fibre quantum channel from affecting the polarization state of the transmitted photons.

This testbed was designed to be robust against externally induced changes in the relative path lengths of the interferometers. During secure key exchange, Bob continually monitored the visibility of his interferometers. Once the QBER exceeded a threshold level, key exchange was halted, and Alice's attenuation was reduced until pulses were transmitted that on average contained more than one photon. At this point, Bob varied the relative path length delay of his interferometers using a piezo-electrically controlled variable length air gap in the delay arms until the visibility was improved. Alice then returned the attenuation to the correct mean photon per pulse level (μ) and key exchange was resumed. In the experiments presented in this paper,

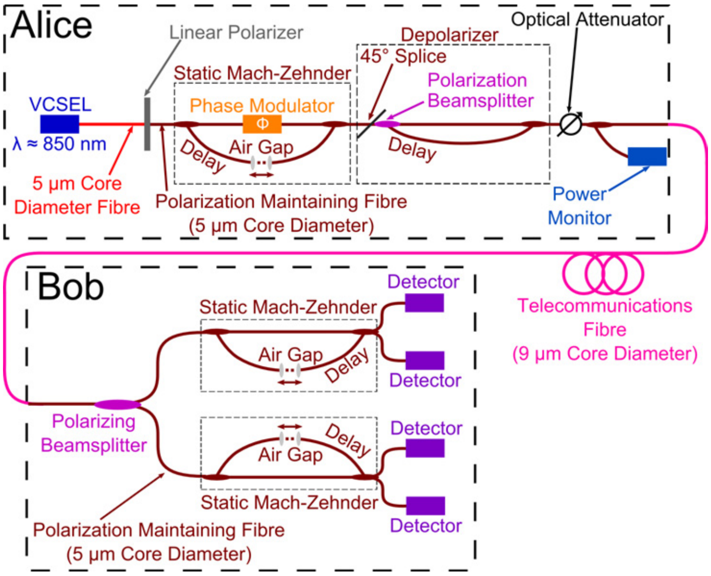

Figure 2. A schematic diagram of the experimental short-wavelength robust QKD system. The air gap in Alice (the transmitter) is fixed for the duration of a measurement, while those in Bob (the receiver) are adjusted under computer control to maintain the maximum fringe visibility in each interferometer. The 9 μm core diameter SMF-28e quantum channel is fusion spliced to the 5 μm core diameter PM fibre used in the construction of Alice and Bob.

a mean of 0.1 photons per pulse was used in all cases. Alice regularly monitored the μ-value launched into the quantum channel and adjusted the attenuation as required to ensure that the μ remained constant. Our system utilized a constant μ of 0.1, meaning that approximately 5% of the non-vacuum pulses leaving Alice contained in excess of one photon. The use of a μ-value with known, controlled variances, decoy states [26], would help us to increase the security of the system and this approach has been demonstrated at GHz clock rates [27].

The current design of the receiver Bob, as shown in figure 2, could potentially allow an eavesdropper to influence the basis set selection by altering the polarization state of the photons [28]. This can be avoided by the introduction of a depolarizer at Bob, which will act to substantially reduce any possible influence. Our measurements have shown that such an all-fibre Lyot depolarizer [29, 30] can be introduced at Bob with a loss of only 1.5 dB. When employed with active monitoring of the coherence length of the incident photons (Eve can, in principle, change the coherence length of the source and reduce the effectiveness of this depolarizing component), Bob would be able to significantly reduce the effectiveness of such an attack [28].

To demonstrate the long-term stability of the QKD system, it was left to run continuously for a period of 24 h fully autonomously and without operator intervention. During this period, the bit rates and QBER were automatically recorded and they are presented in figure 3 for the specific case of the resonant cavity detector. In this set of experiments, a fixed-fibre distance of 2 km was used. The system was operated in enclosed aluminium boxes in a laboratory with air-conditioning, which maintained a constant temperature to ±1° C. During key exchange, the mean QBER was 6.9% and the system was transmitting key for 68% of the 24 h duration of the experiment. The mean sifted bit rate (SBR) calculated after temporal sifting and basis set reconciliation was 60 kbit s^{-1} during the key exchange phases.

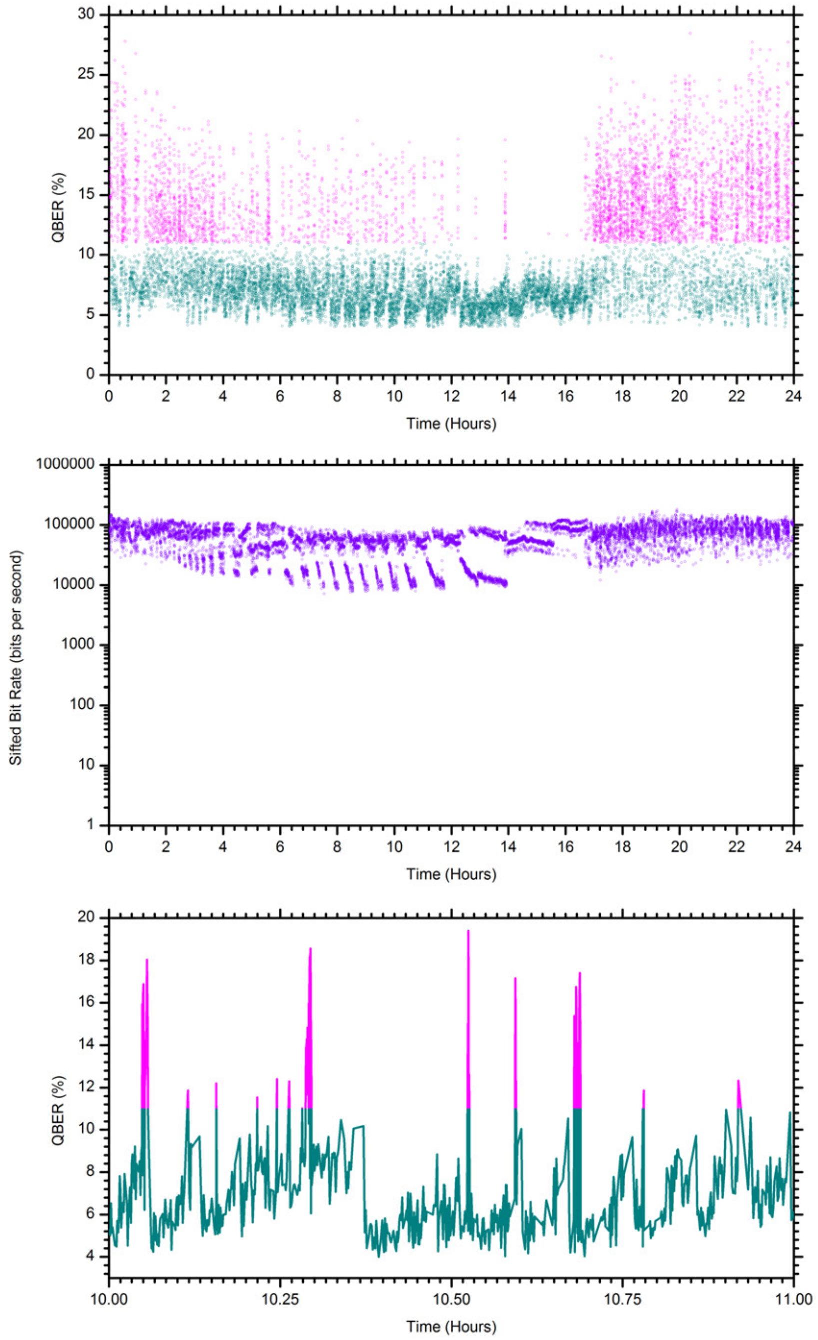

Figure 3. The SBR (middle graph) and QBER (top graph) against time for 24 h fully automated operation of the robust quantum key distribution system using the resonant cavity thin junction Si-SPAD. When the QBER exceeded a threshold value, automatic tuning was initiated, as indicated by the red points in the top graph, and key generation was temporarily halted as the air gaps were adjusted to minimize the QBER. The SBR is shown in the middle graph for the complete operation of the system, including the tuning phase. The bits received during this period would not be used for key generation. The bottom graph shows an expansion of a typical period of operation, in this case the period between 10 and 11 h.

4. Theoretical model

A theoretical model of the system was developed to predict the QBER, raw photon flux recorded by Bob (raw bit rate), the time and basis set sifted photon flux (sifted bit rate) and final key generation rate (net bit rate). Although presented in terms of the experimental QKD testbed described in the previous section, this model can be easily adapted for use with any QKD system.

The raw bit rate (R_{Raw}) can be calculated from the clock frequency (ν), the mean photon number per pulse (μ), the length of the fibre (L_{Fibre}), the per unit attenuation of the fibre ($\alpha_{\text{Fibre}} = 0.603$), the transmission coefficient of Bob ($\alpha_{\text{Bob}} = 0.22$), the detection efficiency of the single-photon detector ($\alpha_{\text{Detection}}$) and the DCR of the detector (R_{Dark}),

$$R_{\text{Raw}} = (\upsilon \cdot \mu) \cdot \left((\alpha_{\text{Fiber}})^{L_{\text{Fiber}}} \cdot \alpha_{\text{Bob}} \cdot \alpha_{\text{Detection}}\right) + R_{\text{Dark}}. \tag{1}$$

This calculation can be adapted for a system employing decoy states by replacing the constant μ term with a term that describes the variance in the mean photon number. The SBR after time filtering and a random basis set choice ($R_{\text{Sifted}}(\Delta T)$) is calculated as

$$R_{\text{Sifted}}(\Delta T) = \alpha_{\text{Protocol}} \cdot R_{\text{Raw}} \cdot I_{\text{System}}(\Delta T), \tag{2}$$

where α_{Protocol} is the protocol loss (which is equal to 1/2 for the BB84 protocol) and ΔT is the duration of the gate used for temporal filtering. $I_{\text{System}}(\Delta T)$ is the fraction of counts that are retained after temporal filtering, which depends on both the duration of the filtering gate and the system detector response function.

$I_{\text{System}}(\Delta T)$ was modelled from an instrument response of the laser output as recorded by the detector and time-stamping electronics. The experimental system is operated at a clock rate of 1 GHz, meaning that for the Si-SPAD detectors, there is still a significant degree of intersymbol interference. We model this by constructing a temporal probability distribution (P_{Arrival}) for the incoming photons based on the instrument response of the system for a particular detector and the four possible paths that a photon may take through the QKD system. In the phase-basis set system presented in this paper, a photon can arrive at the detector having taken one of four cumulative paths: the short arm in Alice & a short arm in Bob, the delay arm in Alice & a delay arm in Bob, the short arm in Alice & a delay arm in Bob or the delay arm in Alice & a short arm in Bob. The first two possible paths do not experience interference, do not contribute to the secure key and may be software time-gated out of the measurement analysis. The detectors presented in this paper could not be hardware gated at a clock rate of 1 GHz. Consequently, they were employed in free running mode and the photon events were software time filtered, or gated, after collection. However, the diffusion tails on the temporal response of the Si-SPAD detectors may cause photons that have taken these non-interfering paths to be detected during the gate assigned to the following interfering path. The time delay between the short and delayed paths in Alice and Bob is set to be 500 ps so that the non-interfering pulses are equally time spaced from the preceding and following interfering pulses. This means that over a periodic signal, the pulses from the short in Alice & short in Bob path are superimposed on those from the delay in Alice & delay in Bob path. It is intersymbol interference resulting from the diffusion tails of photons following the non-interfering paths that limits the maximum clock rate of this system. QKD systems that operate using different techniques for basis set measurements (e.g. those not using matched interferometer delays or those using polarization basis sets) will have a different temporal probability distribution that can be modelled in a similar way.

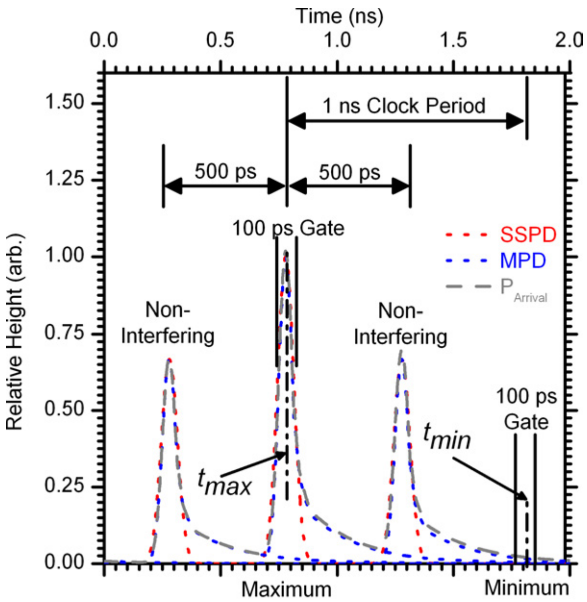

Figure 4. The probability distribution for the theoretical model of the expected arrival time of the photon. The red curves are the results obtained by simulating a histogram of a 1010 repetitive sequence on one SSPD. The blue curves are the individual detector responses for each peak simulated using a MPD detector. The grey curve is the summation of the individual blue MPD detector curves, indicating the intersymbol interference. All curves are created using the piecewise exponential model. The probability distribution is periodic and curves that have not reached zero by the maximum time will re-enter the graph at minimum time and continue to decay until they reach zero. This probability distribution can be adapted for any QKD system by considering the shape of the entire system response over one clock period.

Figure 4 shows P_{Arrival} for a MPD detector and can be considered a probability distribution of the possible times at which a photon from a single pulse may reach the detector. Therefore,

$$I_{\mathrm{System}}(\Delta T) = \frac{1}{\int_0^{2(1/\nu)} P_{\mathrm{Arrival}}\,\mathrm{d}t} \cdot \int_{t_{\mathrm{Max}}-\Delta T/2}^{t_{\mathrm{Max}}+\Delta T/2} P_{\mathrm{Arrival}}\,\mathrm{d}t, \tag{3}$$

where t_{Max} is as defined in figure 4 and P_{Arrival} is defined for a duration of $2(1/\nu)$.

The probability distribution P_{Arrival} is formed using a system instrument response, such as those shown in figure 1. To reduce the effects of noise on the signal, the instrument response was modelled as D_{Response} using a piecewise exponential representation [31],

$$D_{\mathrm{Response}} = \begin{cases} \mathrm{e}^{-(t-t_0)^2/2\sigma^2}, & t < t_1, \\ C_1 \cdot \mathrm{e}^{-t/\tau_1}, & t_1 \leqslant t < t_2, \\ C_2 \cdot \mathrm{e}^{-t/\tau_2}, & t_2 \leqslant t < t_3, \\ C_3 \cdot \mathrm{e}^{-t/\tau_3}, & t_3 \leqslant t < t_4, \\ C_4 \cdot \mathrm{e}^{-t/\tau_4}, & t \geqslant t_4, \end{cases} \tag{4}$$

Table 2. The parameters used in the piecewise exponential fits to the instrument responses shown in figure 1 and the coefficient of determination and goodness of fit of the resulting fits.

Type	Detector	t_1–t_0 (ps)	t_2–t_0 (ps)	t_3–t_0 (ps)	t_4–t_0 (ps)	τ_1 (ps)	τ_2 (ps)	τ_3 (ps)	τ_4 (ps)	σ (ps)
Thick-junction Si-SPAD	PerkinElmer	240	350	636.5	940	151.69	144.15	270.54	603.7	125
Thin-junction Si-SPAD	MPD	36.3	56.3	104.3	626.3	42	83.75	225.64	291.62	21
	IDQ	37	98	668	1070	33	413	1076	1296	20
	Resonant cavity	20	70	120	420	39.63	118.66	270.6	347.96	17
NbN superconducting nanowire	SSPD	–	–	–	–	–	–	–	–	69.5

Type	Detector	C_1	C_2	C_3	C_4	Coefficient of determination, r^2	Goodness of fit, χ^2
Thick-junction Si-SPAD	PerkinElmer	1.5×10^3	2.5×10^3	13	0.25	0.997	1.00
Thin-junction Si-SPAD	MPD	2.7×10^{10}	0.91×10^5	23	4.5	0.998	1.00
	IDQ	1.4×10^{13}	0.85	0.07	0.05	0.946	1.00
	Resonant cavity	3×10^8	2×10^2	2.82	1.1	0.985	1.00
NbN superconducting nanowire	SSPD	–	–	–	–	1.00	1.00

where σ^2 is the variance of the Gaussian region, C_1, C_2, C_3 and C_4 are multiplicative constants, t_0 is the time of the maximum count return in the peak and t_1, t_2, t_3 and t_4 are the points at which the transitions between functions occur. These values are calculated using an iterative Levenberg–Marquardt algorithm [32]. The SSPD was modelled using the Gaussian term alone, without the necessity of the exponentials that define the diffusion tail. The fits resulting from this model are shown by dashed lines in figure 1 and the fitting parameters are shown in table 2.

To derive P_{Arrival}, the piecewise fit D_{Response} was plotted at each of the possible time periods at which a photon could arrive at a detector with the amplitude dependent on the relative loss of the path taken, as shown in figure 4 for the MPD Si-SPAD (blue). The simulated trace from a SSPD (red) is shown for indicative purposes. P_{Arrival} then is the summation of the different overlapping D_{Response} functions for a particular detector, as indicated by the grey dashed line in figure 4 for the MPD-Si-SPAD. P_{Arrival} is periodic and detector tails exiting the graph at $2(1/\nu)$ re-enter at zero time. It is the function P_{Arrival} that will change the most for different QKD systems and it may be developed for any QKD system at any clock frequency using a method similar to that presented here.

The definition of P_{Arrival} given in figure 4 considers perfect interferometric visibility and therefore perfect destructive interference at time t_{Min}. Any counts observed in the temporal gate between $t_{\text{Min}} - (\Delta T/2)$ and $t_{\text{Min}} + (\Delta T/2)$ are, provided ΔT is short relative to the clock period, caused by intersymbol interference.

Calculation of a final secure bit rate requires calculation of the QBER. In a generic QKD system, the QBER can be expressed as containing contributions from the decoding of the quantum states (measurement at Bob), errors in the encoding of the states at Alice, the dark counts of the detector and the timing jitter of the complete system,

$$\text{QBER}_{\text{Total}} = \text{QBER}_{\text{Decoding}} + \text{QBER}_{\text{Encoding}} + \text{QBER}_{\text{Dark}} + \text{QBER}_{\text{Jitter}}. \tag{5}$$

Each term can be calculated from the known characteristic parameters of the system, allowing a final QBER to be computed.

In the system presented in this paper, the term $\text{QBER}_{\text{Decoding}}$ is caused by the classical visibility of the interferometers that make up Alice and Bob and can be expressed as [1]

$$\text{QBER}_{\text{Decoding}} = \frac{1 - \vartheta_{\text{Visibility}}}{2}, \tag{6}$$

where $\vartheta_{\text{Visibility}}$ is the classical visibility expressed as a fraction. For our system, this was measured to be 0.98, indicating that the contribution to the QBER from the visibility is 1%. In an optimized system based on double asymmetric Mach–Zehnder interferometers, this contribution can be reduced to less than 0.1% [33]. In a polarization basis set QKD system, this term can be calculated from the extinction ratio of Bob's polarization analysers.

The term $\text{QBER}_{\text{Encoding}}$ defines the contribution to the QBER caused by errors in Alice's encoding of the quantum states on the photons. In our system, this is due to phase jitter in Alice's modulator, which can be modelled as [34]

$$\text{QBER}_{\text{Encoding}} = \frac{1}{\Delta\phi} \int_{-\Delta\phi/2}^{+\Delta\phi/2} \frac{1 - \cos\phi}{2}\, \mathrm{d}\phi, \tag{7}$$

where $\Delta\phi$ is the variation in phase caused by the modulator. The driving electronics for the phase modulator were found to have an amplitude jitter of 354 mV, corresponding to a $\Delta\phi$ of 0.69 rad and a contribution to the QBER from phase jitter of 1%. In a polarization basis set system, this term can be calculated from the polarization jitter in Alice's polarization modulator if an active scheme is used or the extinction ratio of her polarizers if a passive scheme is utilized.

The contribution to the total QBER caused by the DCR of the detector becomes more significant at longer transmission distances when the photon flux reaching Bob is greatly reduced. This contribution can be calculated via

$$\text{QBER}_{\text{Dark}} = \frac{(1/2) \cdot \alpha_{\text{Protocol}} \cdot \upsilon \cdot \Delta T \cdot R_{\text{Dark}}}{R_{\text{Sifted}}\,(\Delta T)}. \tag{8}$$

Calculation of $\text{QBER}_{\text{Jitter}}$ requires the model developed in figure 4. The value for $\text{QBER}_{\text{Jitter}}$ is given by the ratio of the probability of finding a photon in the gate around the minimum (i.e. destructive interference) position to the sum of this probability of finding a photon in the maximum (constructive interference) position,

$$\text{QBER}_{\text{Jitter}} = \frac{\int_{t_{\text{Min}}-\Delta T/2}^{t_{\text{Min}}+\Delta T/2} P_{\text{Arrival}}\, \mathrm{d}t}{\int_{t_{\text{Min}}-\Delta T/2}^{t_{\text{Min}}+\Delta T/2} P_{\text{Arrival}}\, \mathrm{d}t + \int_{t_{\text{Max}}-\Delta T/2}^{t_{\text{Max}}+\Delta T/2} P_{\text{Arrival}}\, \mathrm{d}t}. \tag{9}$$

The theoretical model predicts the best QBER that may be obtained from an experimental system and does not take into account time-varying changes in the alignment, which lead to fluctuations in the observed values of QBER. These fluctuations are inherently unpredictable in nature and the precise QBER at a particular time cannot be calculated. An upper bound on the QBER will occur when the alignment drifts to the point where the phase states are out of phase.

Calculation of the final secure bit rate must take into account the error correction that will be required to generate a final, secure key [35]. The exact fraction of sifted bits used in the generation of the secure key depends on the algorithm employed, but all commonly employed QKD error correction algorithms [36] and security analysis [36] have a strong logarithmic dependence on QBER. From the work of Gottesman, Lo, Lütkenhaus and Preskill (GLLP), the net bit rate (NBR) $R_{\mathrm{Net}}(\Delta T)$ can be calculated as

$$R_{\mathrm{net}}(\Delta T = \left((1-\Delta) - f_{\mathrm{p}} \cdot H_2\,(QBER_{\mathrm{Total}}) - f_{\mathrm{p}} \cdot (1-\Delta) \cdot H_2\left(\frac{QBER_{\mathrm{Total}}}{1-\Delta}\right)\right) \cdot R_{\mathrm{Sifted}}(\Delta T), \quad (10)$$

where $H_2(x)$ is the binary entropy function [38] given by

$$H_2(x) = -x \cdot \log_2(x) - (1-x) \cdot \log_2(1-x), \quad (11)$$

f_{p} is the efficiency of the error correction protocol relative to the Shannon limit (for the CASCADE error correction protocol [36], f_{p} has a value of 1.16) and Δ is the fraction of pulses intercepted by an eavesdropper. In our analysis, this is given by

$$\Delta \approx \frac{\mu^2}{2} \quad (12)$$

for a weak coherent pulsed source. This analysis does not consider the photon number splitting attack but could be easily adapted to do so.

5. Analysis of detector parameters

The parameters used for the piecewise exponential fits on the instrument responses are listed in table 2. The parameter t_0 defines the peak position of the instrument response at 1 ns, so the transition points are quoted in table 2 with respect to this parameter.

The single-photon detectors at Bob can be replaced with alternative fibre-connectorized detectors, as required. Figure 5 shows the lowest experimentally recorded QBER and corresponding NBR for the five different detectors employed. The dashed lines in figure 5 show the results of the theoretical model when applied to the five detectors and quantifies the quality of the theory model. Table 3 shows the contribution to the total QBER due to jitter. The shape of the QBER graph is primarily determined by the timing jitter profile, the DCR and the detection efficiency 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 the thin-junction SPADs. The instrument responses of the thick-junction Si-SPAD show an FWHM of 432 ps in comparison with ∼67 ps for the thin-junction Si-SPADs. Consequently, there is a greater possibility of photons being time tagged in an incorrect window, thereby increasing the QBER. If the instrument response is considered as a probability distribution of arrival time for the photon, then it can be seen that a longer FWHM timing jitter will have a greater effect on the QBER than a longer FW10%M. Using detectors with comparable FWHM timing jitters, a longer FW10%M will lead to an increase in QBER. The higher baseline QBER obtained using the IDQ Si-SPAD in comparison with the MPD Si-SPAD, which both have a similar FWHM, is

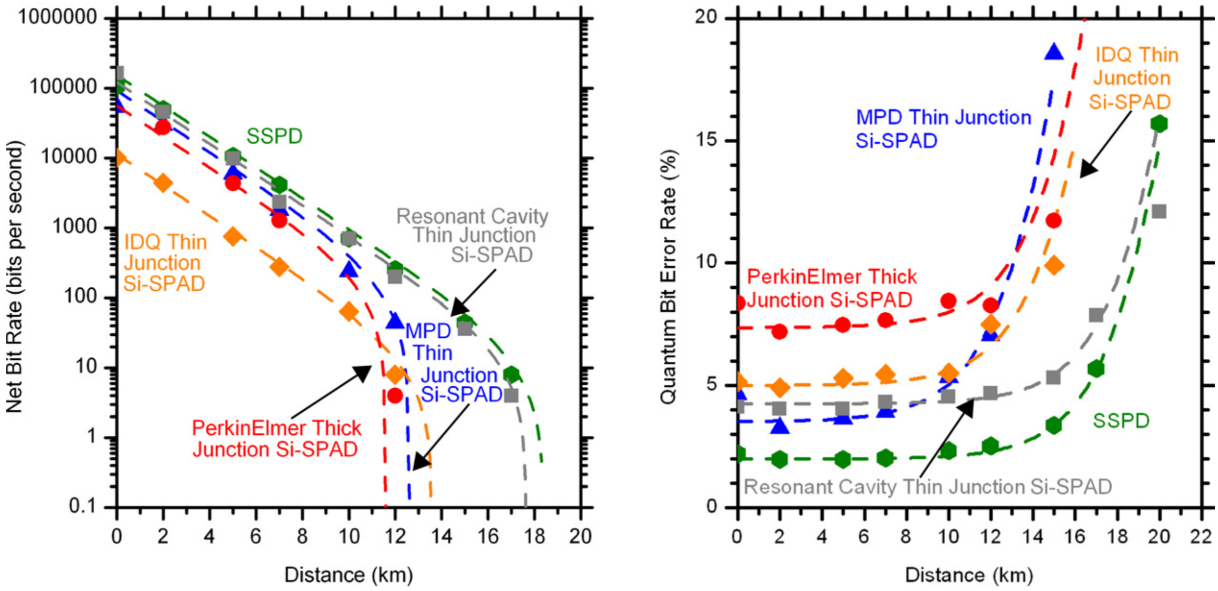

Figure 5. The lowest QBER and corresponding NBR obtained using the five detectors. The dashed lines show the predictions made by the theoretical model, which only considers the best QBER and does not include time-dependent fluctuations.

Table 3. The QBER due to detector timing jitter ($\mathrm{QBER_{Jitter}}$) for the detectors presented in this paper.

Type	Detector	$\mathrm{QBER_{Jitter}}$ (%)
Thick-junction Si-SPAD	PerkinElmer	6.0
Thin-junction Si-SPAD	MPD	2.9
	IDQ	2.5
	Resonant cavity	3.3
NbN superconducting nanowire	SSPD	0.0

partially due to the longer FW10%M and partially due to the much lower detection efficiency of the IDQ detector of 1.6% compared with the MPD detector efficiency of 8.4%. Although they both have similar FWHM jitter, the resonant cavity Si-SPAD exhibits a baseline QBER of 4%, while the SSPD exhibits a baseline QBER of 2%. This is mainly due to the tail present in the temporal response of the resonant cavity Si-SPAD, which is completely absent in the SSPD response.

Following the standard basis set reconciliation defined in the BB84 protocol to produce the sifted key, the detected photon events are temporally filtered to reduce the effect of dark counts using a gate of 100 ps duration centred on the most probable detection time. The left graph in figure 5 shows transmission distance-dependent variation in NBR for each of the detectors. The increased detection efficiency of 18% for the resonant cavity Si-SPAD compared with 10% for the SSPD means that the NBR for the resonant cavity Si-SPAD was higher than that achieved with the SSPD.

Table 4. The effect of altering the FWHM timing jitter of a PerkinElmer thick-junction Si-SPAD. $I_{\mathrm{System}}(\Delta T)$ is the scaling factor from the raw bit rate (which does not change with FWHM) to the sifted bit rate, and can be seen from equation (2). The resulting QBERs and NBRs are shown in figure 7. ΔT, the duration of the temporal gate, was 100 ps.

FWHM timing jitter (ps)	I_{System} (ΔT)	$\mathrm{QBER}_{\mathrm{Jitter}}$ (%)
432	0.10	6.0
390	0.11	4.6
300	0.12	4.2
250	0.17	2.5

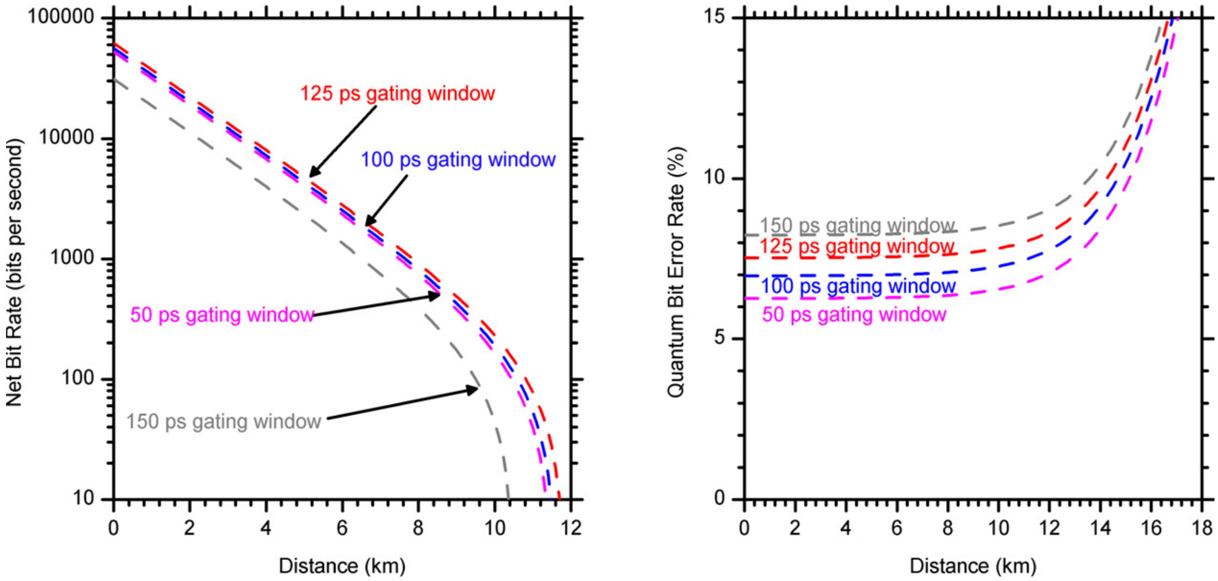

Figure 6. The effect of varying ΔT, the gate duration, on the PerkinElmer thick-junction Si-SPAD.

As a consequence of their lower overall QBER values, the resonant cavity Si-SPAD and the SSPD will give higher secure key exchange rates.

The PerkinElmer thick-junction Si-SPAD has an FWHM timing jitter of 432 ps, which exceeds the ΔT temporal gate duration of 100 ps, and therefore some temporal filtering of the raw detector events occurs. Figure 6 shows the effect of varying the gate duration on both the QBER and NBR. Increasing the gate duration increases the counts within both the $t_{\mathrm{Min}} \pm (\Delta T/2)$ and $t_{\mathrm{Max}} \pm (\Delta T/2)$ temporal windows. Increasing the duration of ΔT increases the effect of intersymbol interference, which leads to an increase in the baseline QBER. In the case of the NBR, an increase in the temporal window increases the counts included in the $t_{\mathrm{Min}} \pm (\Delta T/2)$ and $t_{\mathrm{Max}} \pm (\Delta T/2)$ temporal windows. However, an indefinite increase in ΔT does not necessarily lead to NBR values as the QBER rises with longer ΔT, as observed in the case of the 150 ps temporal window, where the reduction in the NBR is due to the higher QBER for this ΔT.

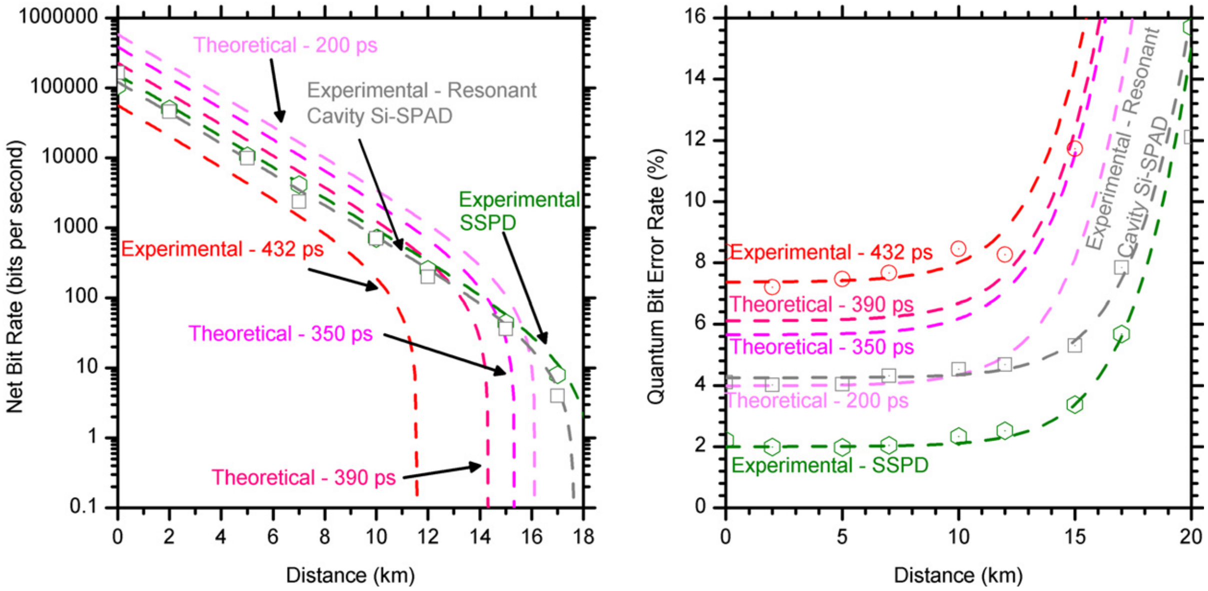

Figure 7. Theoretical model results for a PerkinElmer thick-junction Si-SPAD with identical efficiency and dark count rate, but with varying FWHM durations of 200, 350 and 390 ps. This is compared with the theoretical and experimental results obtained with the detector jitter with the FWHM of 432 ps. The FWHM of 200 ps was chosen as it represents the lowest timing jitter of such a thick-junction detector in a QKD system found in the literature [40]. The grey dotted line indicates the theoretical fit to the experimental results for the resonant cavity thin-junction Si-SPAD and the green dotted line is the theoretical fit for the SSPD. Hollow data points represent the experimentally recorded values for the PerkinElmer thick-junction Si-SPAD with a FWHM timing jitter of 432 ps, the SSPD and the resonant cavity thin-junction Si-SPAD. The variation in $I_{\mathrm{system}}(\Delta T)$ and $\mathrm{QBER}_{\mathrm{Jitter}}$ is shown in table 4.

6. Predictions of future system performance

Previously, it has been shown that the FWHM timing jitter of a PerkinElmer thick-junction Si-SPAD can be reduced by modifying the pulse readout electronics within the detector module [39]. This modified circuit reduced the FWHM of the detector without affecting the DCR or detection efficiency. The shortest unmodified PerkinElmer Si-SPAD FWHM described in the literature, and subsequently used by Restelli *et al* in a previous free-space GHz clock rate QKD system demonstration, was 350 ps, which decreased to 200 ps after circuit modification [40]. This modified detector had a detection efficiency similar to that of the thick-junction detector used in these experiments. The theoretical model was used to calculate the total QBER for this detector, in its initial and modified state, had we been able to use it in our QKD testbed. In modelling the QKD system performance, we have assumed that the detector of Restelli *et al* exhibited the same DCR and τ values as our thick-junction Si-SPAD. We also modelled a further detector with an FWHM jitter of 390 ps, which was chosen as halfway between the FWHM of our unmodified PerkinElmer Si-SPAD and the unmodified PerkinElmer Si-SPAD of Restelli *et al* [40]. The total QBER values are shown in figure 7, along with the experimentally observed total QBER for the resonant cavity thin-junction

Si-SPAD and the SSPD as performance indicators. The FWHM of our unmodified PerkinElmer Si-SPAD is comparable with the time delay of 500 ps between interfering and non-interfering paths introduced by the path length difference in the interferometers. When we decrease the FWHM, the effect of intersymbol interference is lessened, thus lowering the QBER. The detector temporal response affects the baseline QBER, as higher values of the FWHM lead to greater levels of intersymbol interference and a greater contribution to the overall QBER from equation (9). The SBR also increases due to higher probability of photons arriving in the 100 ps time gate. From equation (2), it can be observed that $I_{\text{System}}(\Delta T)$ acts as a scaling factor between the raw bit rate and the SBR and the resultant values are shown in table 4, along with the variation in $\text{QBER}_{\text{Jitter}}$. The grey dotted line in figure 7 shows the theoretical fit to the experimental results for the resonant cavity thin-junction Si-SPAD and the green dotted line shows the theoretical fit to the experimental results for the SSPD.

Thin-junction Si-SPADs typically exhibit long diffusion tails in the instrument response due to carrier pairs being photo-generated outside the detector depletion region and slowly diffusing into the depletion region [5]. It is possible to reduce the duration of these diffusion tails by altering the microstructure geometry. The piecewise exponential model for the system instrument response presented in equation (4) allows us to predict how Si-SPADs with different diffusion tails would affect the performance of the QKD system. For comparison purposes, the thick-junction Si-SPAD was also subjected to the same modelling approach.

The τ values presented in table 2 were scaled to 90, 80 and 70% of the original values to simulate shorter decay tails, and the resulting QBERs and NBRs are shown in figures 8 and 9 respectively. Table 5 shows the parameters of the model as the τ values are changed. When we decrease the duration of the diffusion tail, the contribution to the overall QBER from intersymbol interference ($\text{QBER}_{\text{Jitter}}$ in equation (5)) decreases. This leads to a reduction in the overall modelled QBER and a corresponding increase in the NBR.

A decrease of the diffusion tail fit τ values to 70% of the experimental values lowers the QBER, which could be obtained with the resonant cavity Si-SPAD to the same value as that achieved with the SSPD. The NBR has increased over that which was obtained with the original τ values and is therefore higher than that achieved with the SSPD. A comparison of figures 7 and 9 shows that if the PerkinElmer thick-junction Si-SPAD with a 200 ps FWHM temporal response were to be used in our robust QKD system, it would produce the same net bit rates as a 70% tail resonant cavity thin-junction Si-SPAD with approximately the same QBER at distances of up to 10 km. At distances greater than 10 km, the QBER rises rapidly for 200 ps FWHM PerkinElmer thick-junction Si-SPAD and the NBR suffers a corresponding rapid decrease with transmission distance.

If we make the assumptions that the characteristic parameters of the system, such as the instrument response and uncertainty in the phase state, do not change with the clock frequency, it is possible to model the characteristics of the QKD system for a range of different clock frequencies. Figure 10 shows the result of modelling different clock frequencies for both the SSPD and the resonant cavity thin-junction Si-SPAD when using a 2 km-long quantum channel.

The corresponding decrease in the period of a single bit as the clock frequency increase means that the contribution to the QBER from intersymbol interference increases. The diffusion tail of the resonant cavity Si-SPAD leads to a higher degree of intersymbol interference in comparison with the near-Gaussian instrument response of the SSPD, resulting in a maximum clock frequency of ~1.5 GHz for the resonant cavity Si-SPAD. The SSPD may be utilized at frequencies up to ~5.5 GHz in this system when using a 100 ps duration temporal gating

Table 5. The effect of altering the τ values in the piecewise exponential fit model of equation (4) on the FWHM, FW10%M and FW1%M. $I_{\mathrm{System}}(\Delta T)$ is the scaling factor from the raw bit rate (which does not change with FWHM) and the sifted bit rate, as can be seen from (2). ΔT, the duration of the temporal gate, was 100 ps. The resulting QBER values are shown in figure 8. The resulting NBR values are shown in figure 9.

τ values		100%				90%			
Type	Detector	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	I_{System} (ΔT)	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	I_{System} (ΔT)
Thick-junction Si-SPAD	PerkinElmer	432	837	1473	0.10	424	811	1295	0.10
Thin-junction Si-SPAD	MPD	71	276	898	0.27	68	240	736	0.37
	IDQ	63	193	1245	0.22	63	141	834	0.30
	Resonant cavity	74	271	913	0.22	59	288	964	0.24

τ values		80%				70%			
Type	Detector	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	I_{System} (ΔT)	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	I_{System} (ΔT)
Thick-junction Si-SPAD	PerkinElmer	416	772	1222	0.104	415	765	1154	0.10
Thin-junction Si-SPAD	MPD	65	204	646	0.296	65	168	558	0.31
	IDQ	63	135	522	0.486	63	134	430	0.50
	Resonant cavity	61	227	815	0.28	71	159	629	0.32

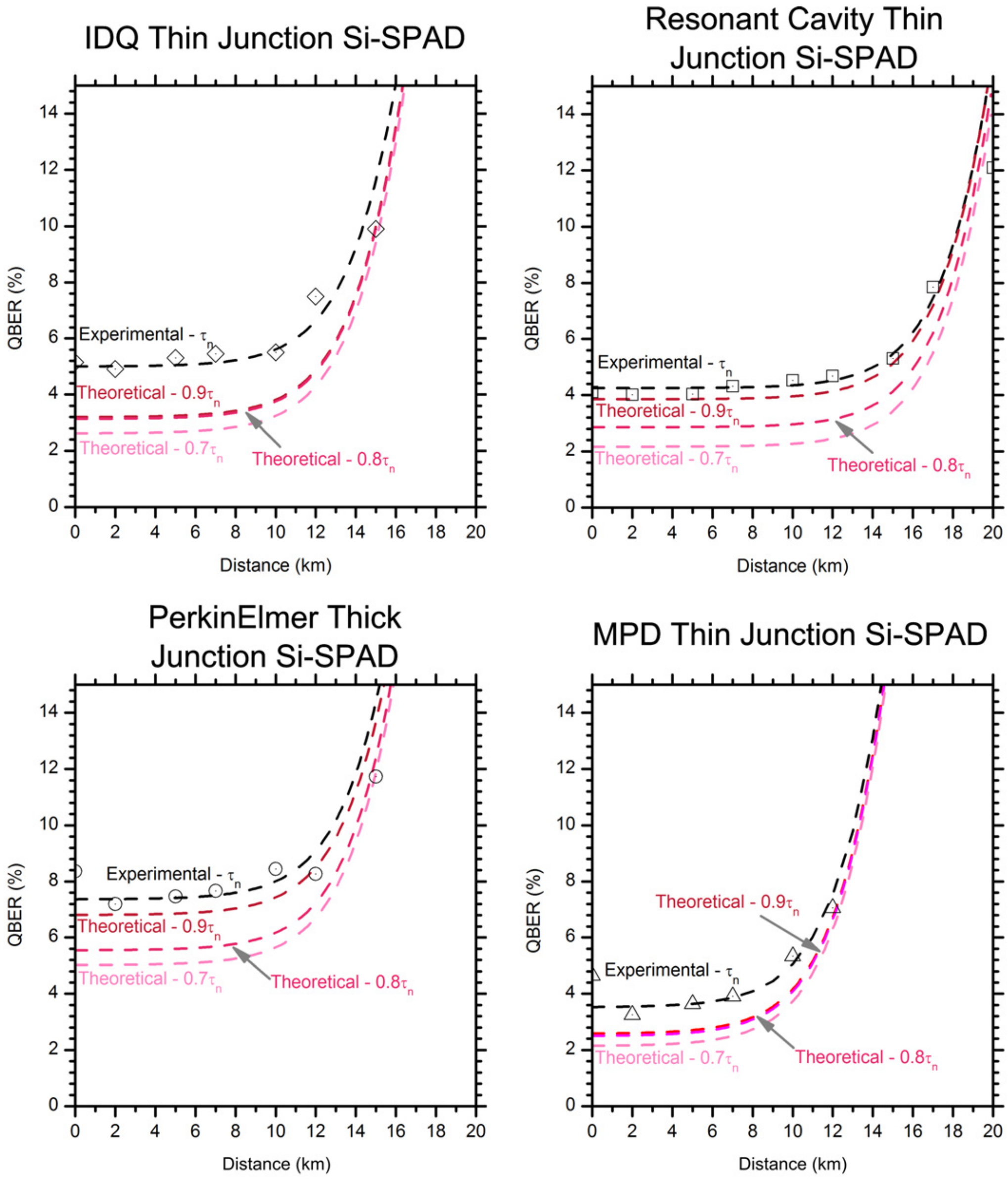

Figure 8. Results from the theoretical model showing the effects on the QBER of altering the decay tails of the instrument responses of the Si-SPADs by changing the τ values in the piecewise exponential fit model of equation (4). The τ values were reduced relative to the values quoted in table 2, as denoted by the scaling factors.

window. The approximately Gaussian temporal response of the SSPD means that shorter temporal gate durations can be used and results have been calculated for a 75 ps gate. With the reduced gate, the maximum clock frequency for the resonant cavity Si-SPAD increases slightly to ∼2 GHz, whereas for the SSPD it increases to ∼6.5 GHz. The baseline QBER values are reduced for both detectors with shorter temporal gate durations. Demonstrations of QKD using SSPDs have been made at clock frequencies up to ∼10 GHz using a 50 ps gating window [3]. The narrow FWHM timing jitter of the SSPD means that there is minimal intersymbol interference and a reduction in the duration of ΔT does not dramatically increase

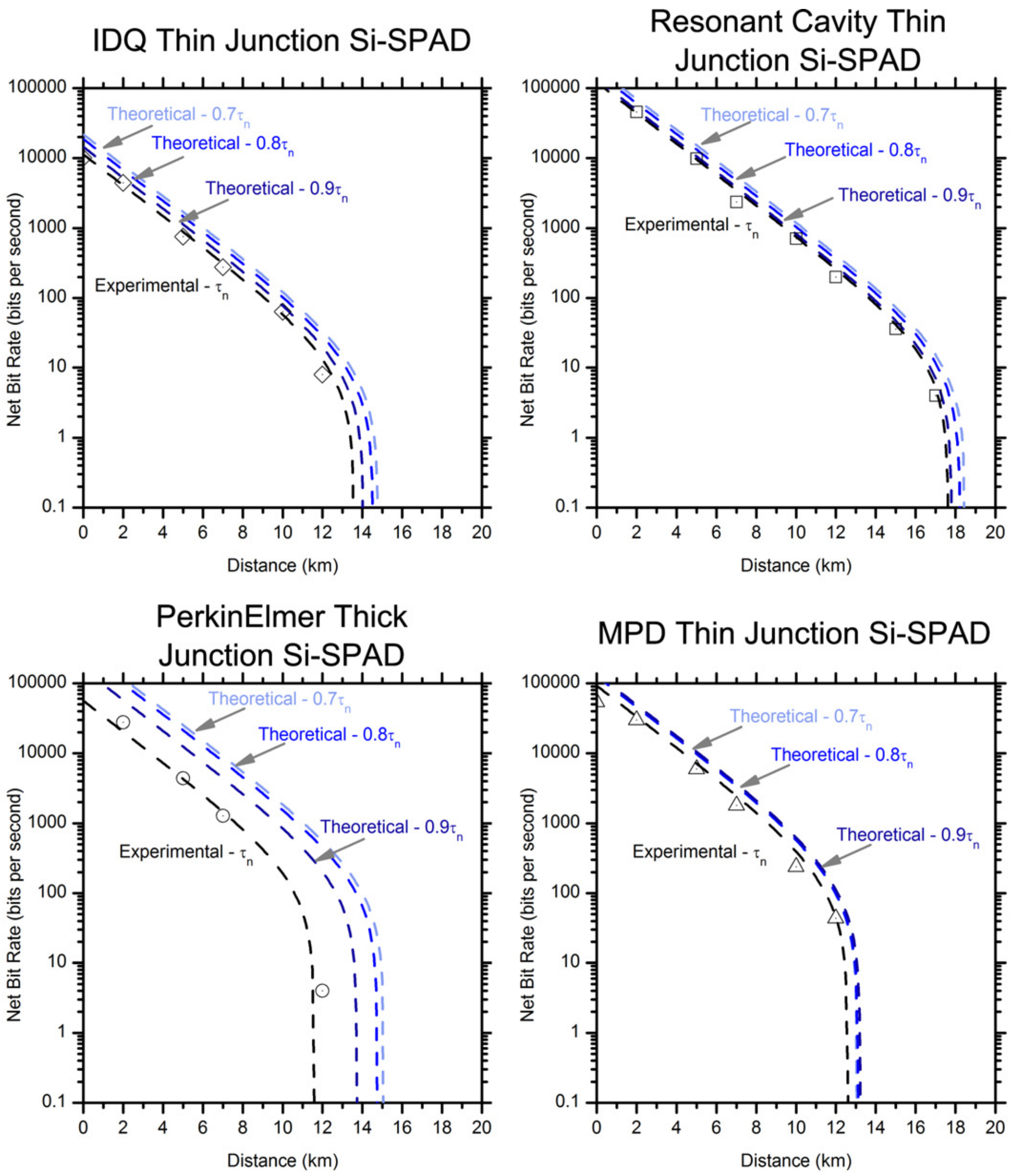

Figure 9. Results from the theoretical model showing the effects on the NBR of altering the decay tails of the instrument responses of the Si-SPADs by changing the τ values in the piecewise exponential fit model of equation (4). The τ values were reduced relative to the values quoted in table 2, as denoted by the scaling factors.

the QBER. Therefore, a reduction in ΔT reduces the $\int_{t_- -(\Delta T/2)}^{t_- +(\Delta T/2)} P_{\mathrm{Arrival}}\, \mathrm{d}t$ term in equation (3), leading to a reduction in the sifted (and hence net) bit rates.

7. Conclusions

We have developed an environmentally robust QKD system that operates at a clock rate of 1 GHz using the BB84 protocol with phase encoding on 850 nm wavelength photons transmitted

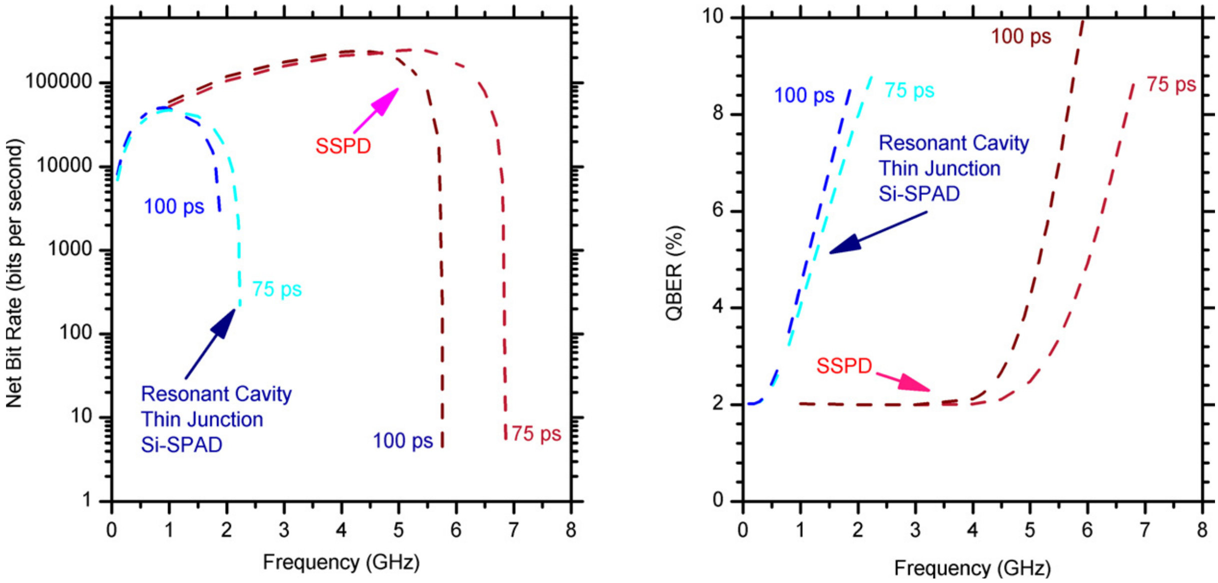

Figure 10. A theoretical prediction of the effects of changing the clock frequency of the QKD system.

through standard telecommunications optical fibre. The use of a QKD system operating at a wavelength of 850 nm has permitted the experimental testing of the model with five different detectors, including the first application of a resonant cavity thin-junction Si-SPAD to QKD. A general theoretical model was developed and applied to the different detectors in the experimental configurations before it was used to predict the behaviour of the system with hypothetical realistic detectors and expected evolutions of existing detectors. This model can be easily adapted for other QKD systems; for example, those operating in optical fibre at a wavelength of 1550 nm or even in free-space by altering equations (6) and (7), which concern the errors introduced by encoding and decoding the quantum states, and specifically by substituting the relevant system instrument response in the calculation of P_{Arrival}.

The Peltier-cooled experimental resonant cavity thin-junction Si-SPAD has been shown to exhibit sifted bit rates that are comparable with the closed-cycle refrigerator-cooled SSPDs. Continuous operation of the system for periods of 24 h has been demonstrated using the resonant cavity thin-junction Si-SPADs, demonstrating that the system is capable of long-term unsupervised operation.

The theoretical model predicts that for the 1 GHz clock rate phase-basis set encoded robust QKD system presented in this paper, if PerkinElmer thick-junction Si-SPADs with 42% detection efficiency, 198 dark counts per second and pulse read-out electronics modified to give a FWHM timing jitter of 200 ps were to be utilized as the detectors, the NBR achieved would exceed that of 62 ps FWHM timing jitter SSPDs with 10% detection efficiency and ten dark counts per second at distances of up to 15 km. This advantage only occurs because the clock frequency of the QKD system is 1 GHz. At higher clock frequencies, intersymbol interference increases the QBER that could be obtained with the PerkinElmer thick-junction Si-SPAD and reduces the net bit rate.

It should be noted that these experiments employed single-layer meander SSPDs [12]. Cavity-embedded SSPDs have been reported with an enhanced intrinsic efficiency of 57% at a wavelength of 1550 nm, with practical efficiencies in excess of 20% at these wavelengths also being reported [41–44]. It is possible that future-generation SSPD devices could be developed to match the 850 nm operating wavelength of this system, yielding improvements in both bit rate and transmission range.

In addition to modifications in the structure of the detectors, it is possible to increase the operating clock rate and key generation rate of QKD systems by utilizing different optical designs. Differential phase-shift QKD systems [45] can reach 10 GHz clock rates [46]. A single photon is transmitted from Alice to Bob in a superposition of three different phase states. The single photons are prepared at Alice and individually transmitted with equal probability into three arms. This system will also exhibit the non-interfering peaks visible in our system but has been operated at 10 GHz clock frequencies with secure key generation rates of 17 kbit s^{-1} over 105 km of fibre using SSPDs [3].

Acknowledgments

The authors gratefully acknowledge financial support from the UK Engineering and Physical Sciences Research Council under projects EP/E003729/1 and EP/F048041/1. RHH was supported by a Royal Society University Research Fellowship. The team from Heriot-Watt University are affiliated to the Scottish Universities Physics Alliance (SUPA). PDT acknowledges support from Science Foundation Ireland under grant no. 06/IN/I969. MG acknowledges funding from EC grant agreement 248095 (Q-ESSENCE) FP7-ICT-2009-4.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95

[2] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28

[3] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors *Nat. Photonics* **1** 343–8

[4] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2010 Continuous operation of high bit rate quantum key distribution *Appl. Phys. Lett.* **96** 161102

[5] Buller G S and Collins R J 2010 Single-photon generation and detection *Meas. Sci. Technol.* **21** 012002

[6] Gordon K J, Fernandez V, Townsend P D and Buller G S 2004 A short wavelength gigahertz clocked fiber-optic quantum key distribution system *IEEE J. Quantum Electron.* **40** 900–8

[7] Fernandez V, Collins R J, Gordon K J, Townsend P D and Buller G S 2007 Passive optical network approach to gigahertz-clocked multiuser quantum key distribution *IEEE J. Quantum Electron.* **43** 130–8

[8] Meyer-Scott E, Hübel H, Fedrizzi A, Erven C, Weihs C and Jennewein T 2010 Quantum entanglement distribution with 810 nm photons through telecom fibres *App. Phys. Lett.* **9** 031117

[9] Choi I, Young R J and Townsend P D 2010 Quantum key distribution on a 10Gb/s WDM-PON *Opt. Express* **18** 9600–12

[10] Collins R J *et al* 2010 Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source *J. Appl. Phys.* **107** 073102

[11] Intallura P M, Ward M B, Karimov O Z, Yuan Z L, See P, Shields A J, Atkinson P and Ritchie D A 2007 Quantum key distribution using a triggered quantum dot source emitting near 1.3 μm *Appl. Phys. Lett.* **91** 161103

[12] Clarke P J, Collins R J, Hiskett P A, Townsend P D and Buller G S 2011 Robust GHz fiber quantum key distribution *Appl. Phys. Lett.* **98** 131103

[13] Bienfang J C *et al* 2004 Quantum key distribution with 1.25 Gbps clock synchronization *Opt. Express* **12** 2011–6

[14] Gordon K J, Fernandez V, Buller G S, Rech I, Cova S D and Townsend P D 2005 Quantum key distribution system clocked at 2 GHz *Opt. Express* **13** 3015–20

[15] Dautet H, Deschamps P, Dion B, MacGregor A D, MacSween D, McIntyre R J, Trottier C and Webb P P 1993 Photon counting techniques with silicon avalanche photodiodes *Appl. Opt.* **32** 3894–900

[16] Ghioni M, Armellini G, Maccagnani P, Rech I, Emsley M K and Ünlu M S 2009 Resonant-cavity-enhanced single photon avalanche diodes on double silicon-on-insulator substrates *J. Mod. Opt.* **56** 309–16

[17] McCarthy A, Collins R J, Krichel N J, Fernández V, Wallace A M and Buller G S 2009 Long-range time-of-flight scanning sensor based on high-speed time-correlated single-photon counting *Appl. Opt.* **48** 6241–51

[18] Krichel N J, McCarthy A, Rech I, Ghioni M, Gulinatti A and Buller G S 2011 Cumulative data acquisition in comparative photon-counting three-dimensional imaging, *J. Mod. Opt.* **58** 244–56

[19] Collins R J, Hadfield R H, Fernandez V, Nam S W and Buller G S 2007 Low timing jitter detector for gigahertz quantum key distribution *Electron. Lett.* **43** 180–182

[20] Tanaka A *et al* 2008 Ultrafast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronisation *Opt. Express* **16** 11354–60

[21] SPCM-AQR single photon counting module Perkin Elmer Datasheet 2005 http://optoelectronics.perkinelmer.com/content/Datasheets/DTSSPCMAQRH.pdf

[22] MPD PDM series Micro Photon Devices Datasheet 2008 http://www.microphotondevices.com/media/pdf/PDM v3 3.pdf

[23] IDQ id100 series IDQ Datasheet 201 http://www.perkinelmer.com/ph/Category/Category/cat1/IDSMI_TAXONOMY_DELETIONS/cat2/IND_SE_CAT_Single%20photon%20Counting%20Modules%20SPCM_001/key/10613

[24] Miki S, Fujiwara M, Sasaki M, Baek B, Miller A J, Hadfield R H, Nam S W and Wang Z 2008 Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates *Appl. Phys. Lett.* **92** 061116

[25] Radebaugh R 2004 Refrigeration for superconductors *Proc. IEEE* **92** 1719–34

[26] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901

[27] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate *Opt. Express* **16** 18790–7

[28] Lo H-K, Qian L and Qi B 2011 private communication

[29] López-Higuera J M 2002 *Handbook of Optical Fibre Sensing Technology* (Wiley-Blackwell)

[30] Burns W K and Moeller R P 1983 Measurement of polarization mode dispersion in high-birefringence optical fibers *Opt. Lett.* **8** 195–7

[31] Pellegrini S, Buller G S, Smith G, Wallace A M and Cova S 2000 Laser based distance measurement using picosecond resolution time-correlated single photon counting *Meas. Sci. Technol.* **11** 712–6

[32] Wallace A M, Ye J, Krichel N J, McCarthy A, Collins R J and Buller G S 2010 Full waveform analysis for long-range 3D imaging laser radar *EURASIP J. Adv. Signal Process.* **2010** 896708

[33] Gobby C, Yuan Z L and Shields A J 2004 Quantum key distribution over 122 km of standard telecom fiber *Appl. Phys. Lett.* **84** 3762–4

[34] Yuan Z L and Shields A J 2005 Continuous operation of a one-way quantum key distribution system over installed telecom fibre *Optics Express* **13** 660–5

[35] Brassard G and Salvai L 1994 Secret key reconciliation by public discussion *Lect. Notes Comput. Sci.* **765** 410–23

[36] Grönberg P 2005 Key reconciliation in quantum key distribution Sensor Technology Technical Report FOI-R-1743-SE Totalförsvarets Forskningsinstitut ISSN 1650-1942

[37] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Quantum Inf. Comput.* **4** 325–60, arXiv:quant-ph/0212066v3

[38] Shannon C E 1948 A mathematical theory of communication *Bell Syst. Tech. J.* **27** 379–423, 623–56

[39] Rech I, Labanca I, Ghioni M and Cova S 2006 Modified single photon counting modules for optimal timing performance *Rev. Sci Instrum.* **77** 033104

[40] Restelli A, Bienfang J C, Clark C W, Rech I, Labanca I, Ghioni M and Cova S 2010 Improved timing resolution single-photon detectors in daytime free-space quantum key distribution with 1.25 GHz transmission rate *IEEE J. Sel. Top. Quantum Electron.* **16** 1084–90

[41] Hu X, Zhong T, White J E, Dauler E A, Najafl F, Hereder C H, Wong F N C and Berggren K K 2009 Fiber-coupled nanowire photon counter at 1550 nm with 24% system detection efficiency *Opt. Lett.* **34** 3607–9

[42] Tanner M G *et al* 2010 Enhanced telecom wavelength single-photon detection with NbTiN superconducting nanowires on oxidised silicon *Appl. Phys. Lett.* **96** 221109

[43] Miki S, Takeda M, Fujiwara M, Sasaki M and Wang Z 2009 Compactly packaged superconducting nanowire single-photon detector with an optical cavity for multichannel system *Opt. Express* **17** 23557–64

[44] Miki S, Yamashita T, Fujiwara M, Sasaki M and Wang Z 2010 Multichannel SNSPD system with high detection efficiency at telecommunication wavelength *Opt. Lett.* **35** 2133–5

[45] Inoue K, Waks E and Yamamoto Y 2003 Differential-phase-shift quantum key distribution using coherent light *Phys. Rev.* A **68** 022317

[46] Takesue H, Diamanti E, Langrock C, Fejer M M and Yamamoto Y 2006 10-GHz clock differential phase shift quantum key distribution experiment *Opt. Express* **14** 9522–30