# Quantum key distribution system clocked at 2 GHz

**Karen J. Gordon, Veronica Fernandez, Gerald S. Buller**

*School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, UK, EH14 4AS*
*k.j.gordon@hw.ac.uk*

**Ivan Rech, Sergio D. Cova**

*Dipartimento Elettronica e Informazione, Politecnico di Milano, 20133, Milano, Italia*

**Paul D. Townsend**

*Photonics Systems Group, Department of Physics, University College Cork, Cork, Ireland*

*http://www.phy.hw.ac.uk/resrev/photoncounting/index.html*

**Abstract:** An improved quantum key distribution test system operating at clock rates of up to 2GHz using a specially adapted commercially-available silicon single-photon counting module is presented. The use of an enhanced detector has improved the fiber-based quantum key distribution test system performance in terms of transmission distance and quantum bit error rate.



**OCIS codes:** (060.0060) Fiber optics and optical communications; (030.5260) Photon counting

## References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. Of IEEE Inter. Conf. on Computer Systems and Signal Processing, Bangalore, Kartarna, (Institute of Electrical and Electronics Engineers, New York, 1984), 175-179.
2. P.W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett. **85**, 441-444 (2000).
3. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," New J. Phys. **4**, 41.1-41.8 (2002).
4. C. Gobby, Z. L. Yuan and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. **84**, 3762-3764 (2004).
5. J. G. Rarity, P. R. Tapster and P. M. Gorman, "Practical free-space quantum key distribution over 10km in daylight and at night," J. Mod. Phys. **48**, 1887-1901 (2001).
6. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity, "A step towards global key distribution," Nature **419**, 450-450 (2002).
7. K. J. Gordon, V. Fernandez, P. D. Townsend and G. S. Buller, "A short wavelength gigahertz clocked fiber-optic quantum key distribution system," IEEE J. Quantum Electron. **40**, 900-908 (2004).
8. J.C. Bienfang, A.J.Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, C.W. Clark, C.J. Williams, E.W. Hagley, J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," Opt. Express **12**, 2011-2016 (2004).
9. C.H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," Phys. Rev. Lett. **68**, 3121-3124 (1992).
10. P. D. Townsend, "Experimental investigation of the perfromance limits for first telecommunications-window quantum cryptography systems," Photon. Technol. Lett. **10**, 1048-1050 (1998).
11. S. D. Cova, M. Ghioni, F. Zappa, "Circuit for high precision detection of the time of arrival of photons falling on single photon avalanche diodes," US pat. 6,384,663 B2, May 7, 2002; (prior. 9 March 2000)
12. I. Rech, I. Labanca, M. Ghioni, S. Cova, "Circuit for improving the photon-timing performance of Single-Photon Counting Modules," (submitted to) Rev. Sci. Instrum.
13. A. Spinelli, A. L. Lacaita, "Physics and Numerical Simulation of Single Photon Avalanche Diodes", IEEE Trans. Electron. Devices **44**, 1931-1943 (1997).

#6089 - $15.00 US Received 17 December 2004; revised 31 March 2005; accepted 5 April 2005

14. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330-1333 (2000).
15. C. H. Bennett, G. Brassard, J. M. Robert, "Privacy amplification by public discussion," SIAM J. Comp, **17**, 210-229 (1988)
16. M. Ghioni, S. D. Cova, A. Lacaita and G. Ripamonti, "New silicon epitaxial avalanche diode for single-photon timing at room temperature," Electron. Lett. **24**, 1476-1477 (1988).

## 1. Introduction

Quantum key distribution (QKD) enables two parties, Alice and Bob, to share a verifiably secure encryption key, guaranteed by the laws of quantum mechanics [1,2].

Since its first experimental implementation in 1992, the growth towards practical applications has been rapid, both in the use of optical fibers as the transmission medium [3,4], and in free-space transmission systems [5,6]. Whilst much experimental effort has been made to increase the transmission span of such point-to-point systems (currently demonstrated at up to ~120km [4]), the key exchange rate still remains low in such systems – typically <1kbits$^{-1}$. This is particularly true in the case of 1.55μm wavelength QKD systems due to count rate limitations imposed by the deleterious effects of the afterpulsing phenomenon evident in the cooled InGaAs/InP single-photon avalanche diode (SPAD) detectors used. In contrast Si SPAD technology is relatively mature and these detectors, which exhibit negligible afterpulsing effects, have been used to increase the potential key exchange rates for campus- or metropolitan-scale networks both in standard telecommunications fiber [7] and in free-space systems [8].

In this paper, we present a modification of the QKD system described in [7] to include an electronically enhanced commercially-available silicon single-photon counting module (SPCM), allowing faster clock rates to be employed. We show that the use of the enhanced module in the QKD system enables the capability of operating up to 2GHz clock rates. The system was characterized in terms of quantum bit error rate (QBER), as discussed previously in [7].

## 2. Description of the system

The gigahertz QKD system, previously described in detail in [7], utilized the B92 protocol [8], which requires only two non-orthogonal states. This protocol was achieved by using two linear polarization states, 45° apart with respect to each other. Alice (transmitter) and Bob (receiver) are primarily constructed from 850nm single mode fiber (SMF), which has a core diameter of ~5μm. However, Alice and Bob are separated using standard telecommunications SMF (as shown in Fig. 1) as the main transmission medium, which has a core diameter of ~9μm and exhibits bi-moded behavior at a wavelength of 850nm [10].

Two vertical-cavity surface-emitting lasers (VCSELs) were used at Alice as the sources of the two linearly polarized encoding states. The VCSELs were driven using two independent laser driver circuit boards, which enabled single mode operation when driven under the correct conditions (< 7mA drive current). The laser driver boards were driven using a non-return to zero (NRZ) differential output from a preprogrammed pulse pattern generator (PPG). The polarized outputs from the VCSELs were launched into 850nm single mode fibers (core diameters of ~5μm) and a pair of polarization controllers were used to set the polarization states in the two channels to linear with a relative polarization angle of 45°. The two fiber channels were multiplexed together using a 2×1 fiber coupler, as shown in Fig. 1. In order to reduce the probability of more than one photon occurring in any pulse period, the output from the 2×1 coupler was attenuated to achieve an average number of approximately 0.1 photons per pulse. The VCSELs were temperature tuned to have identical emission wavelengths of 850nm in order to avoid spectral interrogation by an eavesdropper.

#6089 - $15.00 US Received 17 December 2004; revised 31 March 2005; accepted 5 April 2005

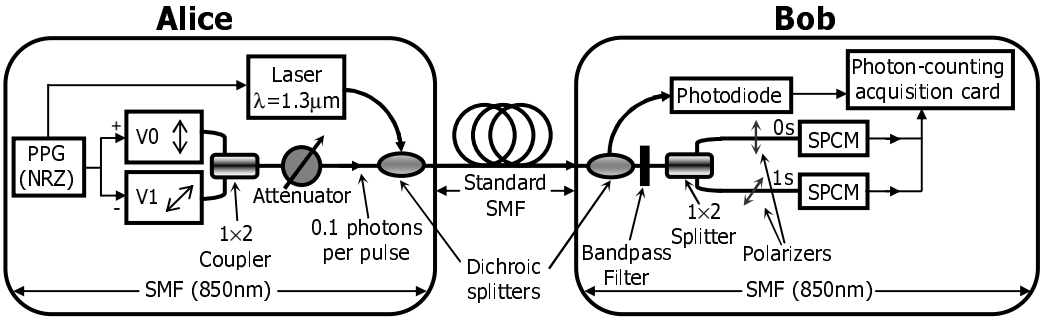


Fig. 1. Basic quantum key distribution system experimental arrangement. PPG: Pulse pattern generator, NRZ: Non return to zero pulse pattern, V0 & V1 are the high-speed VCSELs and driver boards, SPCM: Single-photon counting module, SMF: Single mode fiber.

The system was optically synchronized using intense pulses (~$1.5\times10^8$ photons per pulse) generated by a 1.3μm wavelength distributed feedback (DFB) laser, which were wavelength multiplexed into the fusion spliced transmission fiber connecting Alice and Bob. The two wavelengths were demultiplexed at Bob, and the 1.3μm wavelength pulses were detected by a linear gain germanium avalanche photodiode (APD), whose output was directed to the synchronization input of the photon-counting acquisition card. A bandpass filter ($\Delta\lambda$ = 30nm centered at 850nm) was inserted into the 850nm quantum channel in order to block any remaining 1.3μm wavelength light not removed by the demultiplexer, see Fig. 1. The encoded sequence of photons was randomly routed using a 1×2 splitter, and the polarization discriminated using an appropriately aligned polarizer in each channel.

The 850nm wavelength photons were detected using two commercially-available SPCM-AQR single-photon modules by Perkin Elmer (PKI), one of which was modified for improved performance as described below. The output from the SPCM modules was directed to the photon-counting acquisition card, which can simultaneously acquire data from both channels. Data was then collected using the detected photons and synchronization pulse in order to characterize the system performance in terms of quantum bit error rate (QBER). Only one enhanced SPCM module was available for these measurements, therefore in order to characterize both the 0's and 1's channel using the enhanced detector a measurement was made using one normal SPCM module connected to the 0's channel and the enhanced SPCM module connected to the 1's channel. Once data collection was complete the fiber channels were reversed and the measurement was repeated using the enhanced detector connected to the 0's channel and the normal SPCM module connected to the 1's channel. This allowed a direct comparison with the data taken using the two normal SPCM modules.

### 3. Enhanced detector

The technique described in [11,12] was exploited to improve the photon timing performance of a standard PKI SPCM-AQR photon detector module. An additional circuit card [12] was inserted into the module without modifying the original circuit card, which still quenched the avalanche and could still be used for pulse counting. This modification was reversible and the additional circuit card could be removed with no detrimental effects to the original circuit card. A pulse pick-off linear network was connected to the SPAD terminal, which was biased at a high-voltage (about 400 V). The network was specifically designed to extract a short pulse signal with fast rise, practically coincident with the rise of the avalanche current. A fast discriminator with very low sensing threshold was then employed for sensing the onset of this pulse. Therefore, the avalanche current can be sensed at an initial stage of its build-up, when still confined in a small area of the detector. Thus, the time information obtained was not

#6089 - $15.00 US Received 17 December 2004; revised 31 March 2005; accepted 5 April 2005

affected by the statistical fluctuations that characterize the propagation of the current over the full area of the detector [13]. Hence, the jitter in the measured arrival time of the photon was minimized.

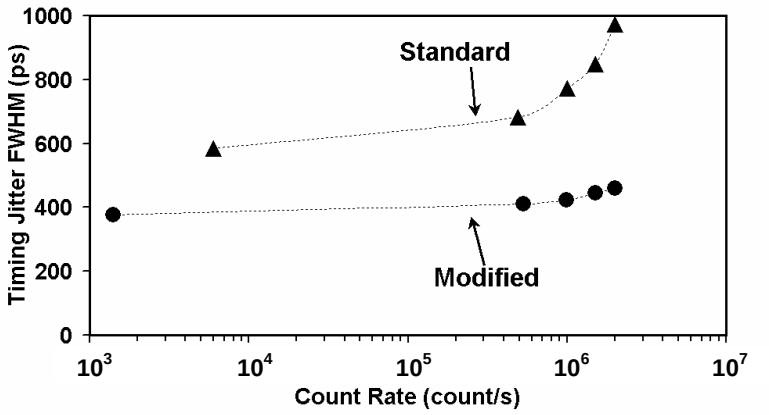


Fig. 2. Timing jitter full width at half maximum of the standard SPCM SPAD and the SPCM with modified output circuitry.

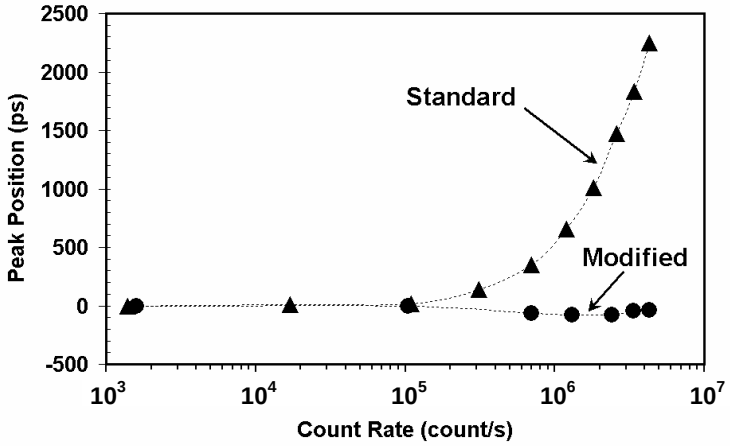


Fig. 3. Shift of the peak position of the standard SPCM SPAD and the SPCM with modified output circuitry.

At low counting rates the original module prior to modification had a full width at half maximum (FWHM) jitter of ~570ps, but with the modification the module had an improved FWHM jitter of ~370ps. The additional circuit card has an added advantage in that its performance was more stable at high pulse counting rates (typically above 0.5Mcounts$^{-1}$). At such rates it is important that the recovery to the baseline level after an avalanche pulse be fast and accurate. If slower tails affect this recovery, even with small amplitude, the superposition of such tails will cause both fluctuations and a systematic mean shift of the baseline level, which causes random fluctuations and shift of the triggering level along the pulse rise time. The corresponding effect on the measured photon arrival time causes a degradation of the FWHM value and a systematic shift of the centroid and of the peak of the photon timing distribution. These effects, which are significant with the original PKI circuit, are strongly reduced by the additional circuit card, as illustrated in Fig. 2 and Fig. 3. For example, at an incident count rate of 2Mcounts$^{-1}$ the modified device exhibits a jitter of ~450ps (FWHM),

#6089 - $15.00 US Received 17 December 2004; revised 31 March 2005; accepted 5 April 2005

compared with ~950ps jitter prior to modification. Temporal broadening of the single-photon detector response has been shown to limit the performance of the QKD system [7] since at clock frequencies between 1 and 2GHz and short fiber lengths the detected count rate can be between 0.5 and 1.5Mcounts$^{-1}$. The reduction in the peak shift does not directly improve the QBER, however it does allow the data collection window to stay fixed with respect to the synchronization pulse [7]. In a high bit rate transmission system this is of fundamental importance, since it means that each bit remains within the proper time slot allotted to it.

**4. Quantum key distribution experimental results**

In this section we show significant improvements in experimental data in terms of QBER by comparing data taken using the standard output of a Perkin Elmer SPCM-AQR photon detector and the output from the additional circuit inserted in the module as described above. There are three main factors that can cause the QBER in the QKD system to increase with increasing clock frequency: (1) broadening and patterning of the VCSEL output pulses due to the limited bandwidth of the laser and associated drive electronics; (2) pulse broadening due to dispersion in the fiber; and (3) the timing jitter of the single-photon detectors at the receiver Bob. The most significant contributor to QBER in the system reported here is the detector timing jitter.

Figure 4 shows the improvement in QBER over a range of high clock frequencies from 1GHz to 2GHz. Comparing the standard SPCM module and the enhanced module for a fixed fiber length of 6.55km the QBER drops below 10% between 1 and 2GHz. This is significant, since a QBER of around 10% is regarded as the threshold value below which a quantum key distribution system can be secure from eavesdropping attacks [14]. The impact of the detector modification is evident: at a clock rate of 2GHz, for example, the QBER halves from the prohibitively high Fig. of ~18% to ~7%, which is below the security threshold. As a result, the estimated net key distribution rate after error correction and privacy amplification [7,15] improves from zero to the order of 20kbits$^{-1}$ at a transmission distance of 6.55km.

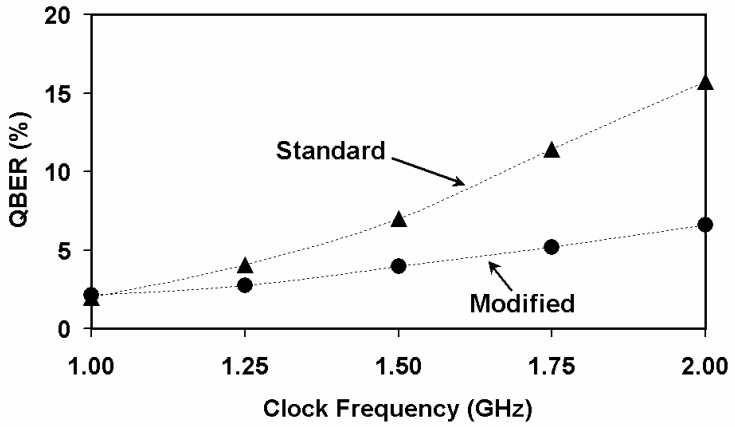


Fig. 4. QBER versus QKD system clock frequency at fixed fiber distance of 6.55 km of standard telecommunications fiber.

The significant improvement at a clock frequency of 2GHz is further illustrated in Fig. 5. Figure 5 shows QBER versus fiber length at a fixed clock frequency of 2GHz. It is clear that the QBER has dropped to a practical level due to the electronic enhancement in the temporal response of the SPCM module. In addition, the marked increase in QBER that is observed at short distances for the standard detector is greatly reduced with the modified detector due to the reduced temporal broadening at high-count rates.

#6089 - $15.00 US Received 17 December 2004; revised 31 March 2005; accepted 5 April 2005

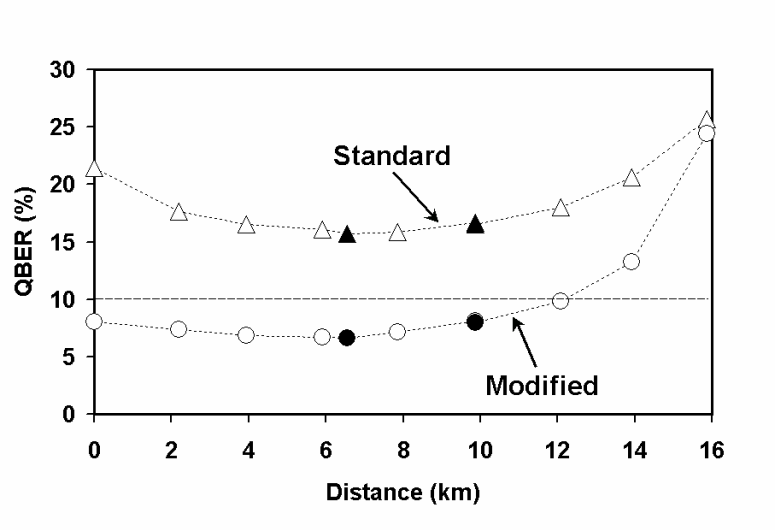


Fig. 5. QBER versus fiber distance at a clock frequency of 2GHz. The points filled in black are taken with the full fiber transmission distance. The white points were measured using optical attenuation to simulate the given distances.

In summary, these results indicate that use of single-photon detectors with a faster temporal response [16] than the SPCM modules currently used in the QKD system, offer the potential benefits of lower QBER and the consequent advantages of longer distance key distribution and/or higher key exchange rates.

## 5. Conclusion

The temporal response of a commercially available single-photon counting module has been significantly improved via a relatively low-cost modification, consisting of the addition of a single dedicated circuit board. The modified detector has been shown to offer important benefits when applied in a QKD system operating at clock rates in excess of 1GHz. Specifically the QKD system has been improved in terms of increased workable clock frequency range from 1GHz to 2GHz, with the results at higher frequencies demonstrating the potential for increased transmission distance. For example, for a fiber length of 6.55km and clock rate of 2GHz the QBER was improved from 18% to 7% leading to an increase in potential key distribution rate from zero to 20kbit/s. Further improvements in source time response and detector timing resolution will further improve system performance, for example the introduction of faster shallow-junction single-photon avalanche diode detectors [16] and higher bandwidth driving electronics and VCSELs.

## Acknowledgments

The authors would like to acknowledge the support of the European Commission SECOQC Integrated Project and the United Kingdom Engineering and Physical Sciences Research Council (project reference GR/N12466). Paul Townsend would like to thank Science Foundation Ireland for support under grant number 03/IN1/1340.