Quantum key distribution at GHz transmission rates

Alessandro Restelli[a,b], Joshua C. Bienfang[a], Alan Mink[a], Charles W. Clark[a]
[a]National Institute of Standards and Technology, Gaithersburg, MD, USA
[b]University of Maryland, Institute for Physical Science & Technology, College Park, MD, USA

ABSTRACT

Quantum key distribution (QKD) channels are typically realized by transmitting and detecting single photons, and therefore suffer from dramatic reductions in throughput due to both channel loss and noise. These shortcomings can be mitigated by applying telecommunications clock-recovery techniques to maximize the bandwidth of the single-photon channel and minimize the system's exposure to noise. We demonstrate a QKD system operating continuously at a quantum-channel transmission rate of 1.25 GHz, with dedicated data-handling hardware and error-correction/privacy amplification. We discuss the design and performance of our system and highlight issues which limit our maximum transmission and key production rates.

Keywords: quantum key distribution, free-space optical communication, single-photon detectors

1. INTRODUCTION

Nearly a quarter of a century after its introduction quantum key distribution (QKD) [1] remains a potential solution to the increasingly demanding problem of cryptographic key distribution over insecure links. Single-photon-based QKD systems have been demonstrated in existing optical-fiber infrastructure [2], and over distances greater than 200 km [3]. However, optical losses in fiber make global-scale fiber-based QKD impractical with current technology. One proposed solution for global-scale QKD is the use of free-space links to a low-earth-orbit (LEO) satellite [4], and recent research has demonstrated success in increasing the distance of free-space QKD links from 10 km [5] to 144 km [6]. Of the numerous technological challenges facing a LEO QKD link, signal loss due to atmospheric turbulence, noise due to background light, and limited access time have been identified as critical issues [4]. Fortunately, each of these challenges appears to be tractable with existing technologies; in this work we focus on the latter two.

When link access times are limited it is beneficial to maximize the key production rate, and recent work has shown that significant improvement can be achieved by increasing the transmission rate of the QKD link [7]. The transmission rate of a single-photon QKD system is typically limited by the temporal resolution of the detectors; a useful figure of merit for the minimum transmission period for low quantum bit error rate (QBER) operation is the single-photon detector's full width at 1% of the maximum (FW1%M). In this article we demonstrate that the temporal resolution of currently available SPADs can also provide a significant improvement in noise reduction. Noise in a free-space QKD link can be reduced with spectral, spatial, and temporal filtering, and while some benefits can be gained by choosing specific operational wavelengths where solar background light is reduced [8], efficient spectral filtering below 0.1 nm remains a technological challenge. However, the full width at half maximum (FWHM) of available SPADs can be significantly lower than the FW1%M. Provided that the signal photons are well localized in each transmission period, the large discrepancy between the FWHM and the FW1%M means that in each transmission period there is a short window in which signal is most likely to be received, and a wider window in which little signal is likely to be received but that is still exposed to random background events. We present a post-selection gating system that takes advantage of this discrepancy to reduce the system's exposure to noise on a free-space channel. The system operates at repetition rates up to 1.25 GHz and is capable of gate widths down to 45 ps.

2. EXPERIMENTAL DESIGN

We implemented QKD with the polarization-encoded BB84 protocol [1] based on attenuated laser pulses. The system runs continuously with a quantum-channel transmission rate of 1.25 GHz and is controlled by two dedicated PCI boards driving both the quantum (single photon) and classical channels. The PCI boards at Alice and Bob each have a field-programmable gate array (FPGA), and two four-channel gigabit Ethernet serializers/deserializers (SerDes): one for the

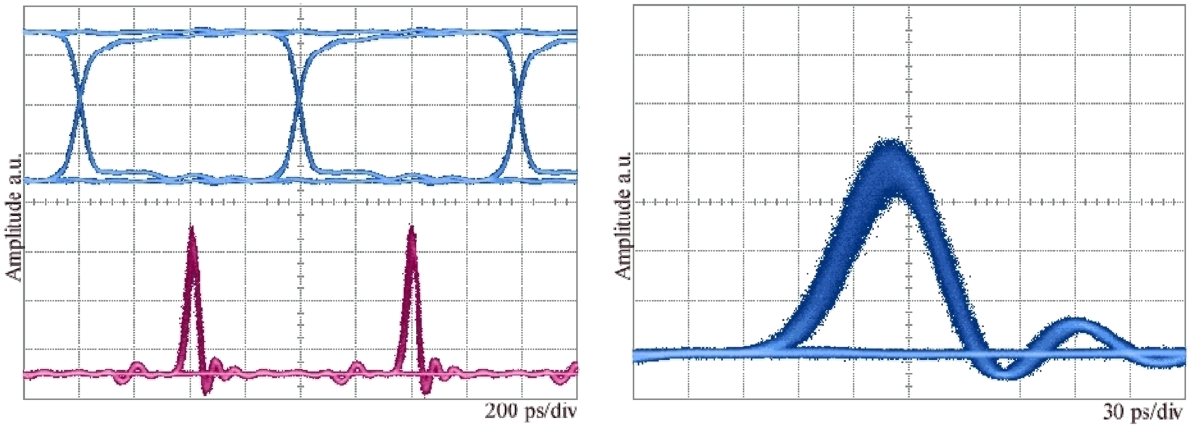
Quantum Communications Realized II, edited by Yasuhiko Arakawa, Masahide Sasaki, Hideyuki Sotobayashi,
Proc. of SPIE Vol. 7236, 72360L · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.809461

classical channel, and one for the quantum channel. The board clock rate is 125 MHz and the four SerDes operate on 10-bit words, resulting in 1.25 Gbps on each serial data channel. On the primary classical channel we use 8B/10B encoding [9] to transmit a balanced 1.25 Gbps serial data stream to which the classical-channel SerDes at Bob can lock an internal phase-locked loop (PLL), thus synchronizing Alice and Bob over the classical channel. Sifting [1] is performed in the FPGA, and both boards communicate with the CPU via a standard PCI interface with direct memory access. This provides a manageable data rate to the CPU for error correction, privacy amplification and application-level data encryption. Further details of the operation of the two PCI boards are presented in ref [7]

Each of the four quantum channel outputs of Alice's PCI board drives a vertical-cavity surface-emitting laser (VCSEL) at 850 nm. The VCSELs are coupled, via single-mode fiber, to free-space optics mounted on the back of the transmit telescope where they are collimated, polarized in either the vertical/horizontal or circular left/right state, and then combined with a non-polarizing beam-splitting cube (NPBSC). The wavelengths of the four VCSELs are temperature tuned to the receiver's 0.15 nm FWHM interference filter centered at 851.4 nm.

A variable attenuator along the path reduces the optical pulse intensity at the output of the telescope to a mean-photon number, $\mu = 0.1$, in each pulse. The transmitted mean-photon number is monitored with a calibrated photon counting module that collects one of the output beams of the NPBSC.

To successfully operate at high transmission rates without generating errors due to timing jitter it is important to minimize the timing uncertainty in the quantum channel. While the detector timing jitter ultimately limits the maximum operational transmission rate of a system, we find that when operating a QKD system with attenuated gain-switched lasers care must also be taken to ensure that pattern-dependent effects do not contribute undue jitter and amplitude fluctuations in the optical output of each transmitter.



(a) (b)

Fig. 1.(a) The upper trace shows one of the four 1.25 GHz NRZ electrical signals from Alice's PCI board used to drive the quantum channel transmitters. The lower trace shows the resulting optical output from the gain-switched VCSEL observed with a 10 GHz photodiode. The optical output shows a clear and open "eye." (b) shows the same optical signal on a shorter time scale, demonstrating that pattern-dependent jitter is negligible.

To minimize pattern-dependent effects in our system we find it effective to drive the VCSELs with short pulses with large amplitude. We use custom electronics to convert the non-return to zero (NRZ) signals from the PCI board to 80 ps pulses with 2.2 V amplitude. The NRZ electrical signal from the PCI board, and the resulting optical signal are shown in Fig. 1. Optical-pulse widths below 50 ps are typical for gain-switched VCSELs [10], though achieving such operation with non-repetitive data signals is less straightforward. We find that the optical pulses from the gain-switched VCSELs do not significantly contribute to the overall timing jitter of the system. Figure 2 shows a histogram of photon arrival times when observed with a 50-ps resolution SPAD [11,12]. The combined effects of the optical source and the detector jitter result in a FWHM of 59 ps. Although the VCSEL is below threshold in the "off" state, we find that the low DC-bias voltage applied in the "off" state causes a weak spontaneous emission that limits the optical extinction ratio to the 36 dB that can be seen in Fig. 2.

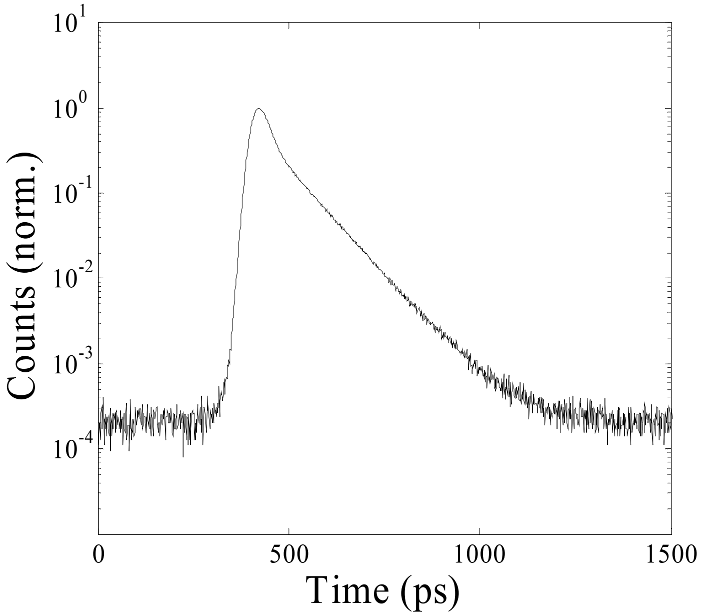


Fig. 2. Histogram of photon arrival time for a VCSEL measured with a 50-ps resolution SPAD. The ratio between the "on" and "off" counts, the optical extinction ratio, can be seen to be 36 dB, limited by spontaneous emission in the SPAD. The detector dark counts (100 counts/sec) are negligible in this data.

At Bob a telescope collects the beam from Alice and a temperature-tuned 0.15 nm interference filter is used to reduce the background light. The necessary random choice of measurement basis is performed by a NPBSC and two pairs of single-photon detectors perform the polarization-state measurement.

In the QKD system we use commercially available SPADs [12,13] with greater than 40 % detection efficiency at 850 nm. These devices were modified with an additional "timing board" designed and fabricated by the Politecnico di Milano [14] that both improves the detector's timing resolution and reduces deleterious count-rate dependent delays. Figure 3 shows a histogram of photon arrival times as measured by one of these detectors. The FWHM of this distribution is 156 ps, well below the 800 ps temporal gate defined by the classical channel.

The performance of the BB84 system over a short free-space link in the laboratory is summarized in Fig. 4. The quantum channel transmission rate is 1.25 GHz. The link loss is changed by adding calibrated neutral-density filters between the transmitter and receiver, and at each value of the link loss the sifted bit rate, the error-corrected and privacy-amplified (EC & PA) bit rate, the quantum-bit error rate (QBER) are recorded. The error-correction algorithm is a hybrid of forward error correction and bisective-search algorithms designed to handle large input sifted bit rates. The necessary degree of privacy amplification is based on a model that considers only individual attacks, and thus is not sufficient for unconditional secret key production [15]. In this article we demonstrate the timing performance and bandwidth limitations of the hardware and data-processing systems in our QKD system as the count rates at the receiver increase; including a more complete threat model requires only software changes. As can be seen in the semi-log plot the bit rates increase linearly with optical link loss, as expected, until about 3.5 dB link loss, where the EC & PA rate reaches 1.05 Mb/s. At this point the CPU (dual-core 3 GHz processor) running the EC & PA algorithm cannot process the incoming sifted bits sufficiently fast and limits the bit production rates. In principle the sifted bit rate continues to increase below 3.5 dB but our system discards the sifted key when the memory is full. The QBER is limited to about 3.1 % by the polarization extinction ratio. We are currently testing new PCI boards in which the error-correction and privacy amplification is performed on the FPGA with a dedicated communications channel, thereby eliminating the CPU from the system. We expect significant improvements in the maximum supported EC & PA bit rates with this system.

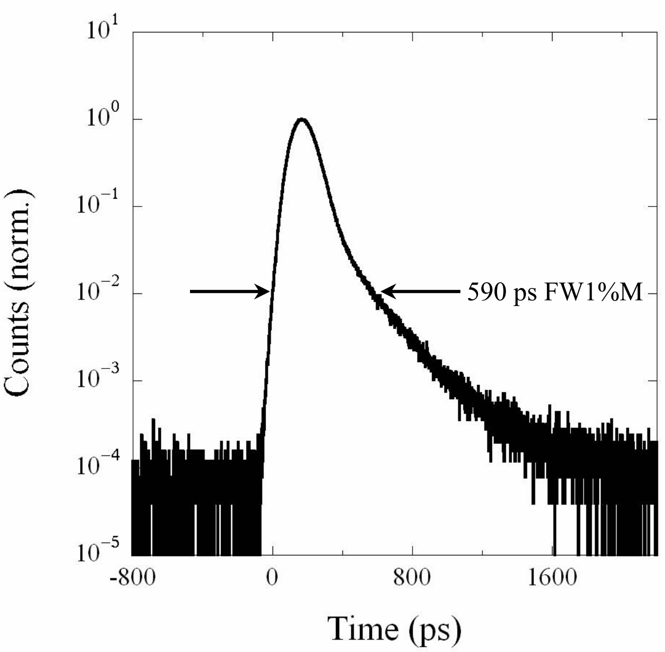


Fig. 3. Timing response of detector with 40% detection efficiency at 850 nm. The modified timing circuit results in a FWHM of 156 ps, FW1%M of 590 ps, and negligible additional jitter at count rates up to 1 Mcounts/s.

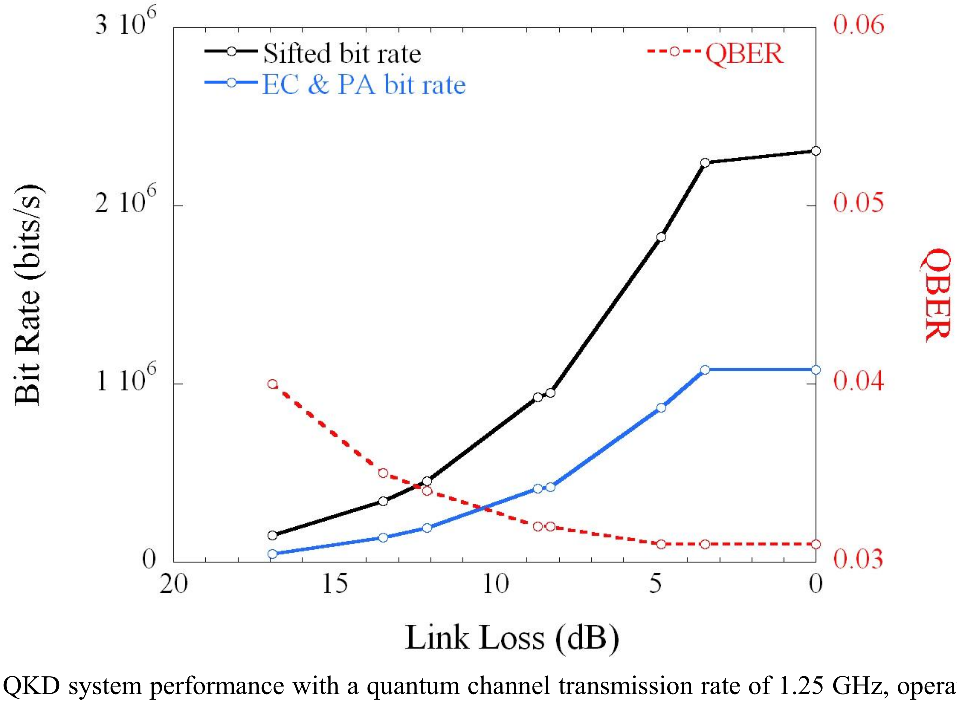


Fig. 4.The QKD system performance with a quantum channel transmission rate of 1.25 GHz, operating over a free-space link in the lab. The CPU running the error-correction and privacy-amplification (EC & PA) algorithms can handle output rates up to 1.05 Mb/s, at which point its buffers fill and the system discards any incoming sifted bits, producing the sharp “kink” at 3.5 dB loss.

To operate with reduced exposure to random background counts, such as those from the sun, we investigate an additional sub-clock gating system used to post-select detection events that occur within a pre-determined temporal window. Extremely high temporal resolution photon counting (< 5 ps) can be achieved with time-tagging systems based on time-to-digital conversion (TDC) [12, 16]. However, such systems require a significant reset time after each detection event and this can limit the system to a rate lower than the maximum count rate of the detectors. Furthermore, every tagged event must be filtered by time-tag comparison, increasing the overall load on the data processing system. An alternative technique is gated photon counting [17]. In this technique an electrical pulse is used to define a temporal gate; detection events that occur outside of the gate are ignored while those that occur within are retained. To be effective with short gate widths it is necessary to have precise knowledge, at the receiver, of the temporal window in which a transmission event will arrive.

Gated photon counting therefore requires that a triggering or synchronization signal be supplied to the receiver. This technique is well suited for our QKD system where clock distribution has been incorporated into the classical-channel architecture. The advantages of gated photon counting are its simplicity and speed: events outside the region of interest are immediately discarded and do not require further processing, and gating pulses with widths below 50 ps and gigahertz repetition rates can be produced with commercially available hardware.

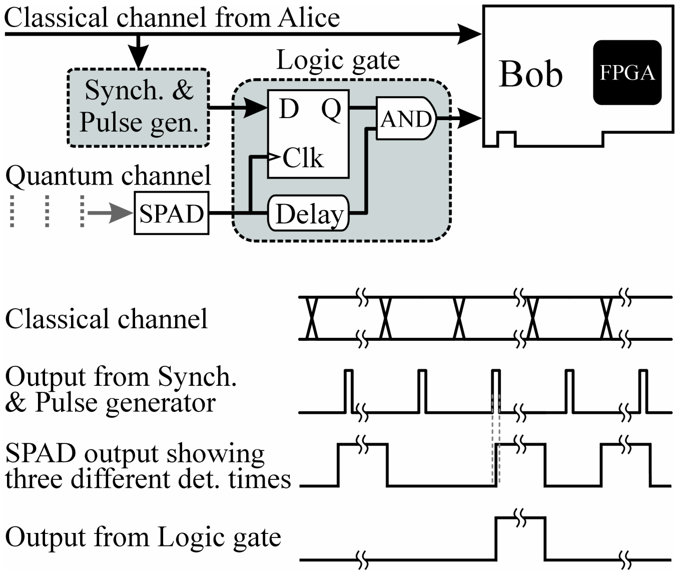


Fig. 5. Schematic of the temporal gating system and associated timing diagram. The synchronization and pulse-generator circuit produces electrical pulses, synchronous with Alice's transmission clock, of width down to 45 ps that are used to gate detection events on the quantum channel. The timing diagram illustrates that only a detection event whose rising edge occurs within the gate defined by the pulse generator is passed through the system. For clarity, only a single quantum-channel receiver and gate system is shown, and for brevity in the timing diagram temporal breaks are used to graphically shorten the SPAD output pulses, which in reality are much longer than a clock period.

Figure 5 shows a schematic of the post-selection gating system, and illustrates the operation of the gate. The system is composed of two blocks: a synchronization and pulse-generation system, and a simple logic system. The synchronization system recovers a stable replica of the QKD transmitter's (Alice's) clock from the classical channel. The pulse generator uses programmable delay chips and gigahertz logic to create a comb of electrical pulses synchronous with the transmission clock, as illustrated in the timing diagram of Fig. 5. These pulses define the temporal gate. The logic system compares the rising edges from SPAD detection events to these gate pulses and blocks events that occur outside of a gate pulse. To optimize performance, the system allows adjustment of the width of the gating pulses, and their phase with respect to Alice's clock, with picosecond accuracy.

The logic system is based on a 10 GHz edge-triggered flip-flop and logic gates. The output from the pulse generator is sent to the data input (D) of the flip-flop. Signals from the SPAD output (i.e. detection pulses) are sent both to the flip-flop clock input (Clk), and through a delay to an AND gate. When a rising edge from a SPAD detection signal arrives at the flip-flop clock input, the logical state at the data input is transferred to the flip-flop output (Q). This output state is then used to enable or disable the transmission of the SPAD signal through the AND gate. To avoid ambiguity at the AND gate it is useful to delay slightly the SPAD pulse to ensure that it arrives at the AND input after the flip-flop output has reached a stable state. With the fast transition times of the gigahertz logic this delay can be implemented by adding extra length to the signal trace on the PCB. The AND gate is specified to add random jitter of the order of 1 ps RMS [12, 18] and we find that the output pulse preserves the temporal position of an input edge with better than 5 ps accuracy, the resolution of our measurements.

The post-selection gating system is demonstrated in Fig. 6, which shows a histogram of ungated detection events at a transmission rate of 1.25 GHz, and the same measurement when a gate of 175 ps is applied. Within the gate the shape of the histogram is indistinguishable from the ungated histogram, indicating that timing information is well preserved. Outside the 175-ps gate the count profile falls off rapidly, with an average slope of 15 ps/decade. This slope is due to detection events that occur at the gate boundary. In the boundary region the electrical pulse that defines the gate is traversing the decision threshold of the flip-flop when the detection edge arrives, causing some uncertainty in the flip-flop output. This uncertainty limits the minimum gate width to roughly 45 ps. Some contribution to these boundary effects also comes from the resolution of our measurement system.

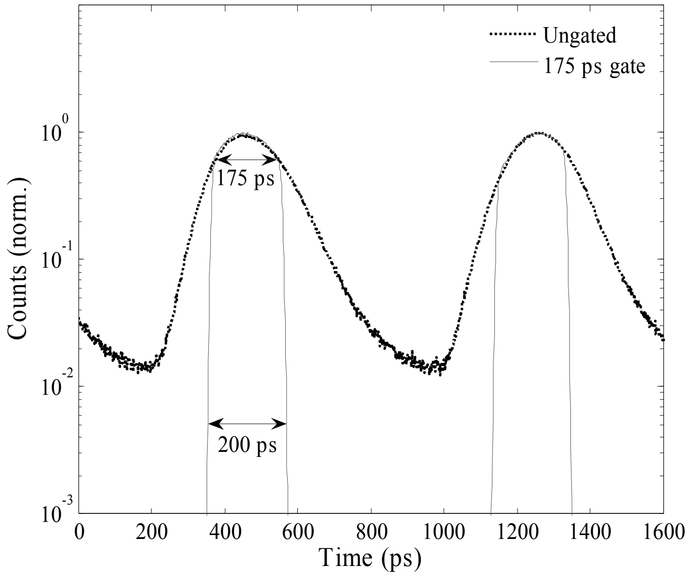


Fig. 6. Histogram of gated and ungated detection events. Detection events that occur outside the 175-ps gate are rejected, while the timing resolution of those that occur within the gate is accurately preserved. The finite slope at the gate boundaries is due to the electronics and causes the full-width of the gated-count profile to increase to 200 ps at a level -20 dB from the count level at the gate.

3. CONCLUSIONS

We have presented a free-space polarization-encoded BB84 QKD system operating with a quantum channel transmission rate of 1.25 GHz. Careful attention to the design of the electronics driving our gain-switched VCSEL sources minimizes the timing jitter due to our optical source, and allows the system to take full advantage of the timing resolution of the single-photon detectors. Furthermore, we have presented a post-selection gating system capable of imposing narrow temporal gates on our detection system that can be used to reduce the system's exposure to background light sources without limiting the repetition rate.

REFERENCES

[1] Bennett, C. Brassard, G., “Quantum Cryptography: public key distribution and coin tossing,” Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175–179 (1984).

[2] Runser, R.J., Toliver, P., McNown, S., Chapuran, T. E., Goodman, M.S., Jackel, J., Hughes, R.J., Nordholt, J.E., Peterson, C.G., Tyagi, K., Hiskett, P., McCabe, K., “Quantum cryptography in optical networks and supporting metrology,” Technical Digest: Symposium on Optical Fiber Measurements, 159-162, (2004).

[3] Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., Lita, A. E., Nam, S. W, Nordholt, J. E., “Long-distance decoy-State quantum key distribution in optical fiber,” Phys. Rev. Lett., 98, 010505-1-4, (2007)

[4] Rarity, J. G., Tapster, P.R., Gorman, P. M., Knight P., “Ground to satellite secure key exchange using Quantum cryptography,” New J. Phys., 4, 82.1-82.21, (2002).

[5] Hughes, R. J., Nordholt, J. E., Derkacs, D., Peterson, C. G., “Practical free-space quantum key distribution over 10 km in daylight and at night,” New J. Phys., 4, 43.1-43.14, (2002).

[6] Weier, H., Schmitt-Manderbach, T., Furst, M, Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik,Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A., Weinfurter, A., “Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144km,” Phys. Rev. Lett., 98, 010504, (2007).

[7] Bienfang, J. C., Gross, A. J., Mink, A., Hershman, B. J. , Nakassis, A., Tang, X., Lu, R., Su, D. H., Clark, C.W., Williams, C. J., Hagley, E. W., Wen, J., “Quantum key distribution with 1.25 Gbps clock synchronization,” Optics Express, 12, 2011-2016, (2004).

[8] Rogers, D. J., Bienfang, J. C., Mink, A., Hershman, B. J., Nakassis, A., Tang, X., Ma, L., Su, D.H., Williams, C. J., Clark, C. W., “Free-Space Quantum Cryptography in the H-alpha Fraunhofer Window,” Proc. SPIE, 6304, 630417-1, (2006).

[9] Widmer A. X. and Franaszek P. A., “A DC-balanced, partitioned-block, 8B/10B transmission code,” IBM J. Res. Develop., 27, 440-451 (1983).

[10] Zhu, B., White, I. H., Williams, K. A., Tan, M. R. T., Schneider, R. P., Corzine, Jr. S. W. and Wang, S. Y., “Ultra low Timing Jitter Picosecond Pulse Generation from Electrically Gain-Switched Oxidized Vertical-Cavity Surface-Emitting Lasers,” IEEE Photonics Technology Letters, 9, 1307-1309, (1997).

[11] Datasheet: Micro Photon Devices srl, PDM Series 100ct single-photon detection module, http://www.microphotondevices.com/media/pdf/PDM_v3_1.pdf (accessed February 15, 2008).

[12] Certain trade names and company products are mentioned in the text or identified in an illustration in order to specify adequately the experimental procedure and equipment used. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

[13] Datasheet: http://optoelectronics.perkinelmer.com/content/Datasheets/DTS_SPCMAQRH.pdf (accessed November 17, 2008).

[14] Rech I., Labanca, I., Ghioni, M., Cova. S. “Modified single photon counting modules for optimal timing performance,” Review of Scientific Instruments. 77, 033104-1-5, (2006).

[15] Gottesman, D.; Lo, H.K., Lutkenhaus N., Preskill, J. “Security of quantum key distribution with imperfect devices,” Quantum Inform. Comput. 4, 325–360, (2004)

[16] Datasheet: Becker & Hickl GmbH, TCSPC General Solution SPC-600/630, http://www.becker-hickl.de/pdf/dbspc6b.pdf (accessed February 15, 2008).

[17] Becker, W., “Advanced Time-Correlated Single Photon Counting Techniques,” Springer-Verlag Berlin Heidelberg: New York, 12-16, (2005).

[18] Datasheet: Inphi GHz logic, Inphi Corp., http://www.inphi-corp.com/product-overview/ghz-logic.php/ (accessed November 17, 2008).