Free-Space Quantum Cryptography in the H-alpha Fraunhofer Window

D. J. Rogers[†], J. C. Bienfang[‡], A. Mink[‡], B. J. Hershman[‡], A. Nakassis[‡], X. Tang[‡], L. Ma[‡], D. H. Su[‡], Carl J. Williams[‡], and Charles W. Clark[‡]

Abstract

Free-space Quantum key distribution (QKD) has shown the potential for the practical production of cryptographic key for ultra-secure communications. The performance of any QKD system is ultimately limited by the signal to noise ratio on the single-photon channel, and over most useful communications links the resulting key rates are impractical for performing continuous one-time-pad encryption of today's broadband communications. We have adapted clock and data recovery techniques from modern telecommunications practice, combined with a synchronous classical free-space optical communications link operating in parallel, to increase the repetition rate of a free-space QKD system by roughly 2 orders of magnitude over previous demonstrations. We have also designed the system to operate in the H-alpha Fraunhofer window at 656.28 nm, where the solar background is reduced by roughly 7 dB. This system takes advantage of high efficiency silicon single-photon avalanche photodiodes with <50ps timing resolution that are expected to enable operation at a repetition rate of 2.5 GHz. We have identified scalable solutions for delivering sustained one-time-pad encryption at 10 Mbps, thus making it possible to integrate quantum cryptography into first-generation Ethernet protocols.

Introduction

Quantum cryptography (QC) is emerging to provide a fundamental shift in the way we approach cryptography. By relying on the quantum mechanical properties of the physical communications layer rather than the mathematical complexity of the communications process for its security, QC, specifically Quantum Key Distribution (QKD), can provide a communications link that is provably immune to eavesdroppers and independent of their technological capabilities.

Generally QKD can be thought of as a simultaneous quantum optics experiment occurring at two different locations, the results of which can provide an encryption key that is statistically random and known only to the two parties involved. The security of the experiment relies on two fundamental properties of quantum mechanics. The first, the indivisibility of individual quanta, is a fundamental principle of quantum mechanics. Wooters and Zurek proved the second idea, the so-called 'no-cloning theorem,' in 1982 [1], which states that an unknown quantum state cannot be cloned without a measurement

[†] Chemical Physics Program, University of Maryland, College Park, MD and National Institute of Standards and Technology, Gaithersburg, MD; drogers2@umd.edu
[‡] National Institute of Standards and Technology, Gaithersburg, MD

Free-Space Laser Communications VI, edited by Arun K. Majumdar, Christopher C. Davis,
Proc. of SPIE Vol. 6304, 630417, (2006) · 0277-786X/06/$15 · doi: 10.1117/12.680899

that risks changing that state. Together these results provide the premise for Quantum Cryptography's 'unbreakable' security.

The Current NIST QKD System

At the National Institute of Standards and Technology (NIST), in Gaithersburg, MD, we have established a QKD Testbed in order to develop and evaluate quantum cryptographic technologies. We have constructed a free-space optical QKD communications link across 730 meters that operates up to 1.0 Mbps [2]. This system has been successfully demonstrated to transmit one-time-pad encrypted streaming video and represents a major improvement in secret (error corrected and privacy amplified) key rate.

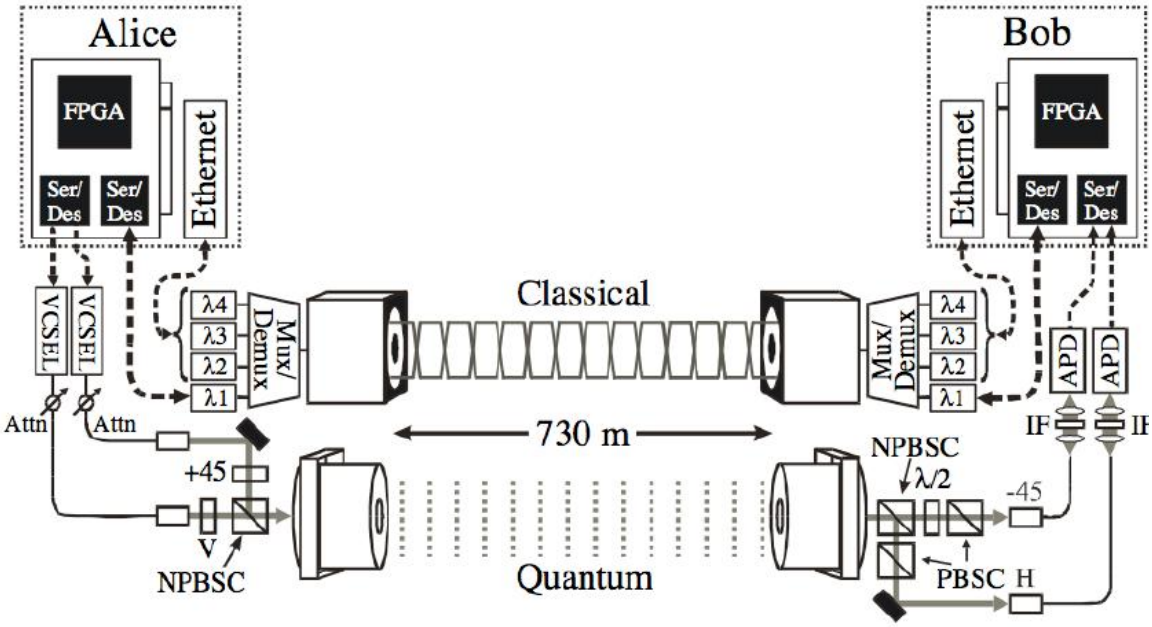

Figure 1 - The NIST B92 Free-Space QKD System

The key to the high bit rate of the NIST system lies in the custom PCI boards and parallel classical optical channel. Each board has a field-programmable gate array (FPGA) and two four-channel gigabit Ethernet serializer/deserializers (SerDes). The two SerDes, one for the primary classical channel and one for the quantum channel, use a 1.25 Gbps data stream on each serial data channel and employ 8-bit/10-bit encoding to transmit a balanced clock signal over the primary classical channel. The scheme allows Bob to synchronize the receiver clock to the transmitter using an internal phase-locked loop (PLL). Using this technique we are able to continuously create 800 ps time bins to gate the quantum channel receiver and thus enable high-speed quantum key transmission in a scalable manner.

The fundamental performance limitation of the current NIST QKD system is the timing jitter in the detector's avalanche photodiodes (APDs). Although we are able to

synchronize the transmitter and receiver clock at 1.25 Gbps, the timing jitter in the detectors limits us to lower clock rates. Figure 2 shows the count distribution of a typical detector. The FWHM of 250 ps and long tail imply that, in order to avoid detection errors due to overlapping time bins, Alice must transmit on alternating clock cycles. This limits the transmission rate to 625 MHz.

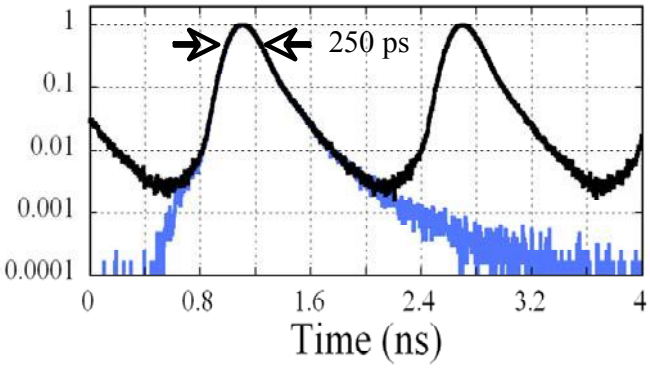

Figure 2 - The current system is limited in transmission speed by the detector timing jitter.

Because we are limited by our detector performance, we are currently fabricating a new free-space QKD system centered on new detectors with improved timing resolution [3].

Improved Single-Photon Detectors

The central components behind the new NIST system are the improved single-photon detectors. These detectors are based on thinner APDs that reduce the timing jitter. The timing resolution of an APD is significantly affected by the thickness of the depletion region of the device. Since the output timing is strongly determined by the time at which the absorbed photon generates the initial carrier, a larger physical volume over which the photon can be absorbed results in a larger statistical distribution of delays between photon arrival and signal onset [4]. The new detectors have, among other improvements, significantly thinner depletion regions and thus decrease the statistical variation in delay. Specifically, the detectors exhibit a timing jitter of 35 ps. The improvement timing resolution is particularly significant in the tail of the histogram, where the full width at 1/100 can be as low as 370 ps [5]. The new detectors should allow for a bin width of 400 ps and a potential transmission rate of 2.5 Gbps – a four-fold improvement over the current system.

Sub-clock Gating

To further improve the system's performance, we are able to localize the pulse to a 100 ps portion of that 400 ps bin, enabling us to gate the receiver at even less than the 400 ps. This sub-clock gating scheme can reduce the exposure to background noise counts by a

factor of four. Some preliminary results showing the implementation of the sub-clock gate are illustrated in Figure 3.

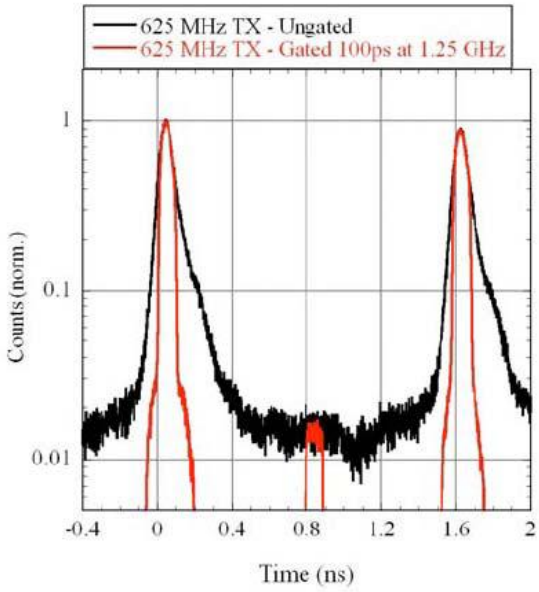

Figure 3 – A Histogram of the ungated APD signal and the post-selected gated APD signal shows a dramatic decrease in background noise counts.

How effectively the gating improves performance is directly related to how accurately the pulse is localized within the bin. The gate not only eliminates noise, but also potentially eliminates signal counts as well. Thus it is important to find an optimal gate time that reduces noise while minimally impacting the signal level. The degree of localization of the pulse is illustrated in Figure 4, showing that nearly the same number of counts occur in the first 150 ps of the bin as occur in the full 400 ps bin.

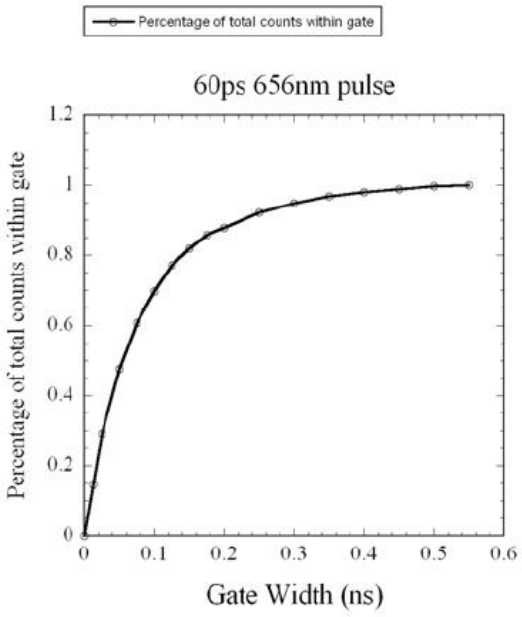

Figure 4 - For gate times greater than 150 ps, over 80% of the signal counts are retained.

QKD in the Visible Spectrum

The other significant effect of the thin absorption region is the wavelength shift of the detector's peak sensitivity. The profile of the extinction depth in Si [6] dictates that the peak sensitivity of thinner APDs will occur at shorter wavelengths when compared to thicker devices. Thus creating a thinner APD will cause its peak absorption wavelength to shift from the near-IR in the older devices into the visible region of the spectrum for the new APDs.

In order to operate in a high efficiency spectral region, the new NIST system is designed around a visible wavelength. However, simply operating at the detector's peak response at 550 nm has the undesired effect of introducing more solar background noise into the receiver. The solar spectrum, roughly a blackbody at 5900 K, has higher emission in the visible region of the spectrum compared to the near-IR. Furthermore, Rayleigh scattering results in more ambient skylight in the visible region. Thus by shifting to a visible wavelength, the new QKD system is potentially susceptible to increased solar background noise and higher error rates.

To avoid this problem of increased solar background noise, we have designed the new system to operate in the H-α Fraunhofer band at 656.28 nm. This wavelength corresponds to the n=2-3 transition in atomic hydrogen, an abundant material in the sun's atmosphere. Atomic hydrogen in the solar photosphere absorbs at this wavelength from the overall blackbody emission. At the same time, atomic hydrogen in the solar chromosphere reradiates at lower intensity at this same wavelength. The net absorption

and radiation results in a 7-8 dB reduction in overall solar irradiance at the H-α wavelength [7].

The H-α line is actually made up of seven broadened fine-structure lines [8]. For this reason it is one of the widest Fraunhofer lines in the solar spectrum and is therefore the easiest to use for free-space optical communications [9]. Filters that are nominally as wide as the band, at 1.2 Å, are commercially available for solar astronomy and are easily adapted to this application. However, the broadening and the finite filter width imply that the system will not be able to take full advantage of the decrease in background noise. We have performed a preliminary experiment using angle tuning of the commercial filters to measure the reduction in background counts from the sun. The results, illustrated in Figure 5, imply that we can expect a 45-60% decrease in solar background noise by incorporating these filters.

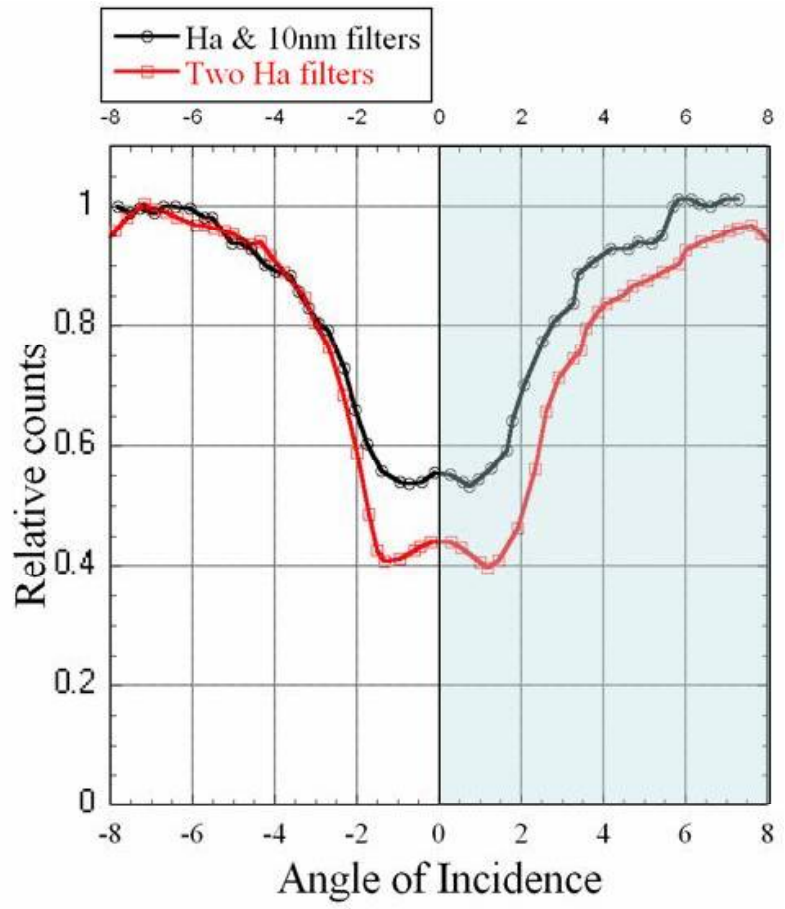

Figure 5 - Commercial Fraunhofer filters provide 45-60% reduction in background counts.

Despite the availability of filters at the H-α wavelength, there are still a number of challenges to making a QKD system in the visible region of the spectrum. Whereas near-

IR systems take advantage of existing telecommunications technology such as Gbps lasers, detectors and good quality optical fiber, equivalent parts at visible wavelengths are either difficult to obtain or simply non-existent. To realize Gbps signaling at visible wavelengths, we are implementing a pulse carving system using a continuous wave, external cavity tunable diode laser and custom-fabricated electro-optic modulators. These modulators suffer from relatively poor extinction ratios. However, despite these impediments, we have successfully created 60 ps pulses at 656.28 nm with a driver capable of a 2.5 GHz repetition rate, as illustrated in Figure 6.

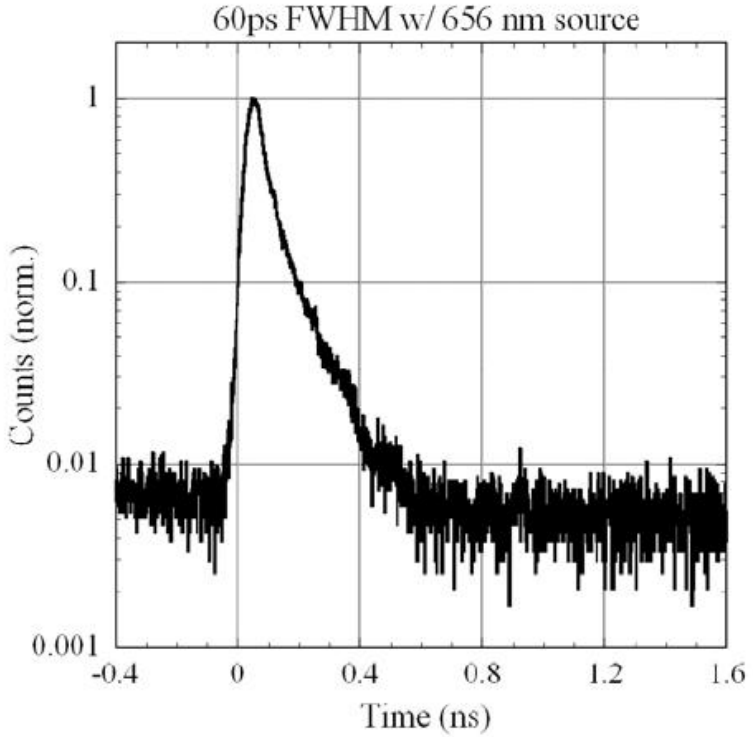

Figure 6 - A count histogram shows 60 ps pulses at 656.28 nm using a pulse-carving scheme.

Performance Projections

Each aspect of the new design will impact the overall secret key rate in a different way. By using the new detectors, we will gain a factor of four in our transmission speed. However, because the new detectors operate at a shorter wavelength with lower efficiency, we will experience reduced signal count rates and increased noise. To counter this effect we are implementing sub-clock gating and carefully choosing our wavelength to reduce the solar background noise. To determine the net effect of all of these design changes, we have constructed a simple analytical model to predict the sifted key rate, quantum bit error rate and final secret key rate.

The equations that describe the statistical behavior of the QKD system integrate a number of parameters, including atmospheric transmittance, direct sunlight and scattered solar (skylight) irradiance, receiver bandwidth and aperture and receiver gate time. The atmospheric parameters were determined using the U.S. Air Force MODTRAN atmospheric transmission modeling software [10]. This software incorporates meteorological conditions, geographic information, atmospheric makeup and transmitter/receiver geometry to determine the atmospheric transmission and skylight irradiance for a specified wavelength range. The results of this model were incorporated into the overall analysis and prediction of our new QKD system.

The first performance metric calculated is the expected sifted key rate, ρ_{sift}, which is given by

$$\rho_{sift} = \frac{\mu \cdot T_{atmos} \cdot \eta}{2\Delta t} + 2D + \frac{R_{sky} \cdot A \cdot \Delta t' \cdot \lambda \cdot \Delta\lambda \cdot \Omega}{2hc\Delta t}$$

where is the mean photon number per pulse, T_{atmos} is the atmospheric transmission, η is the detector efficiency, Δt is the bit period, D is the dark count rate, R_{sky} is the skylight irradiance (determined from MODTRAN), A is the receiver aperture, $\Delta t'$ is the receiver gate time, λ is the transmission wavelength, $\Delta\lambda$ is the filter spectral width and Ω is the solid angle of the receiver's field of view. The first term corresponds to the actual transmitted photons from Alice that make it through the link to Bob and are not sifted out. The second term represents the dark-count rate after sifting, and the third term represents the photons that are detected from the background solar and skylight radiation. Using the sifted key rate, we can then calculate the expected quantum-bit error rate (QBER) using

$$QBER = \frac{D + \dfrac{R_{sky} \cdot A \cdot \Delta t' \cdot \lambda \cdot \Delta\lambda \cdot \Omega}{4hc\Delta t}}{\rho_{sift}}$$

This expression accounts for the bits that are detected but did not originate at Alice. Dividing by the sifted key rate gives us QBER as a percentage of the sifted-key rate, rather than an error count rate.

We have performed empirical software testing of our error correction and privacy amplification algorithm and experimentally determined its throughput rate as a function of the QBER in percent. We have fit the following curve to that data:

$$\rho_{secret} = 2.8 \cdot \exp(-28 \cdot QBER)$$

where the secret key rate, ρ_{secret}, is in Mb/s. Using these expressions and parameters = 0.1 photons/pulse, η = 34%, Δt = 400 ps, D = 750 cps, A = 30 cm^2, λ = 656.28 nm, $\Delta\lambda$ =0.12 nm and an atmospheric visibility of 23 km, we ran the model for various gate times

to determine the effectiveness of the sub-clock gating and to determine the expected performance of the new system. The results of the model are outlined in the table below. Note that the visibility parameter is a standard input parameter to MODTRAN and is used to determine the atmospheric transmission and skylight irradiance.

Gate Width (ps)	Sifted Key Rate (Mb/s)	QBER (%)	Secret Key Rate (MB/s)
400 (ungated)	3.6635	4.10	0.8849
200	3.3040	2.28	1.4749
100	2.4586	1.55	1.8133

The model results indicate two competing effects that influence the final secret key rate. While gating the receiver reduces the detection time and thus the sifted key rate, it has a much stronger impact on the error rate by reducing background counts. In this way gating provides an overall improvement in the secret key rate. As the table shows, we expect to see nearly a two-fold increase in our final secret key rate over the current NIST QKD system.

Conclusion

The current NIST QKD system suffers from limitations due to the timing jitter in the single-photon detectors. By incorporating new detectors, carefully choosing our operating wavelength and implementing gating circuitry in the receiver, we hope to achieve a two-fold increase in our secret key rate. One implication of the increased key rate is an increase in bit-value correlations in the sifted key. This effect becomes apparent in high-speed systems, where the detector count rates approach the detector dead times. For the new detectors, initial simulations indicate correlations on the order of 1%, indicating the need for increased privacy amplification to obtain a secret key. Nonetheless, these improvements will bring the NIST QKD system to a speed that will approach first-generation Ethernet protocols, making it feasible to use multiplexing or other techniques to integrate a fully functional, one-time-pad encrypted QKD system into the existing telecommunications infrastructure.

References

[1] Wooters, W. K. and W. H. Zurek, "A Single Quantum Cannot be Cloned," *Nature*, **299**, 802 (1982).

[2] Bienfang, J. C., A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, C. Clark, C. Williams, E. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," *Opt. Express,* **12**, 2011-2016 (2004).

[3] Cova, S., A. Longoni, and A. Andreoni, "Towards picosecond resolution with single-photon avalanche diodes," *Rev. Sci. Instr.,* **52**, 3 (1981).

[4] Cova, S., M. Ghioni, A. Lotito, I. Rech and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," *J. Mod Opt*., **15**, 9-10, pp 1267-1288 (2004).

[5] Gulinatti, A., P. Maccagnani, I. Rech, M. Ghioni and S. Cova, "35 ps time resolution at room temperature with large area single photon avalanche diodes," *Elec. Lett*., **41**, 5 (2005).

[6] Palik, E. D., ed., *Handbook of Optical Constants of Solids*, Orlando: Academic P. (1985).

[7] Kurucz, R. L., I. Furenlid, J. Brault and L. Testerman, "Solar flux atlas from 296 to 1300 nm," *National Solar Observatory Atlas*, Sunspot, NM: National Solar Observatory (1984).

[8] Reader, J., "Reference Wavelengths for Strong Lines of Atomic Hydrogen and Deuterium," *Appl. Spect.*, **58**, 12, (2004).

[9] Kerr, E. L., "Fraunhofer Filters to Reduce Solar Background for Optical Communications," *TDA Progress Report 42-87*, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA (1986).

[10] http://www.vs.afrl.af.mil/ProductLines/IR-Clutter/modtran4.aspx