LA-UR- 10-06352

Approved for public release;
distribution is unlimited.

Title:	SATELLITE-BASED QUANTUM COMMUNICATIONS
Author(s):	Richard J. Hughes, P-21 Jane E. Nordholt, P-21 Kevin P. McCabe, ISR-4 Raymond Newell, P-21 Charles G. Peterson, P-21
Intended for:	Proceedings of: "Updating Quantum Cryptography and Communications 2010" (UQCC2010) Tokyo, Japan, October 18-20, 2010

Los Alamos
NATIONAL LABORATORY
EST. 1943

Form 836 (7/06)

SATELLITE-BASED QUANTUM COMMUNICATIONS

Richard J. Hughes[1], Jane E. Nordholt[1], Kevin P. McCabe[1], Raymond T. Newell[1], and Charles G. Peterson[1]
[1] *Los Alamos National Laboratory, Los Alamos, NM 87545, USA*

Introduction: Single-photon quantum communications (QC) offers the attractive feature of "future proof", forward security rooted in the laws of quantum physics. Ground based quantum key distribution (QKD) [1] experiments in optical fiber have attained transmission ranges in excess of 200km, but for larger distances we proposed a methodology for satellite-based QC [2]. Over the past decade we have devised solutions to the technical challenges to satellite-to-ground QC, and we now have a clear concept for how space-based QC could be performed and potentially utilized within a trusted QKD network architecture. Functioning as a trusted QKD node, a QC satellite ("QC-sat") could deliver secret keys to the key stores of ground-based trusted QKD network nodes, to each of which multiple users are connected by optical fiber or free-space QC. A QC-sat could thereby extend quantum-secured connectivity to geographically disjoint domains, separated by continental or inter-continental distances. In this paper we describe our system concept that makes QC feasible with low-earth orbit (LEO) QC-sats (200-km-2,000-km altitude orbits), and the results of link modeling of expected performance.

Satellite QC challenges: In the year 2001, our team performed a 10-km ground-based experiment [3] showing that free-space QC can be performed, even in daylight, with sufficient signal-to-noise ratio (SNR) for BB84 QKD across atmospheric paths with optical challenges (extinction, background and turbulence) that are at least as great as on a satellite-to-ground path. The methodology to make this possible uses a wavelength plan and a combination of spectral, spatial and temporal filtering that we invented. Other research groups have since published longer-range results in the less stressing night-time SNR regime [4]. We analyzed LEO-to-ground QC using a link model anchored to the results of our 10-km experiment [5]. Results of satellite QC optical link modeling have since been published by research groups in Europe [6], Japan [7] and China [8]. Together, these results provide evidence for the ultimate feasibility of satellite-to-ground QC. However, a system architecture must be devised that can accommodate multiple additional challenges beyond those present in a static ground-to-ground link. These include: link acquisition and tracking; synchronization and timing; a QC space terminal design that can be space-qualified and accommodated within satellite size, weight and power budgets; and a QKD protocol design that is consistent with the constrained computational and conventional communications resources of a space platform [5]. Security and link availability (in daylight as well as night) are over-arching requirements. Drawing on our team's recent developments in finite-statistics [9, 10, 11] decoy-state BB84 QKD protocols [12], and our recent integration of QC with free-space optical communications (FSOC), we have devised a system concept that permits a QKD session to be completed within a single, few-minute duration, LEO-to-ground optical contact, using modest size optical apertures on the space terminal (5 – 20-cm diameter) and on the ground (~ 50 – 100-cm diameter).

Satellite QC system architecture: Space-to-ground QKD can be accomplished using single-photon polarization qubits, because they experience negligible decoherence or polarization-dependent loss. The required BB84 states can be produced in the QC transmitter ("Alice") using short (< 1ns), highly attenuated pulses of linearly polarized laser light (mean photon number $\mu < 1$), and polarization-analyzed into BB84 states using passive polarization optics in the QC receiver ("Bob") [3]. An architecture in which Alice is located in space and Bob is located on the ground has multiple advantages. There is considerable heritage for lasers in space; the optically disruptive influence of atmospheric turbulence is located in the far-field; a large receiver aperture is simpler to implement on the ground; and the computationally intensive portions of the QKD protocol can be performed on the ground where greater resources are more readily available [5].

Our analysis of secret bit yield as a function of wavelength [5], taking into account single-photon detection efficiencies, atmospheric transmission and background shows that a photon wavelength of ~ 780nm will be optimal, permitting the use of commercially available silicon avalanche photo-diode detectors. With these detectors and typical receiver apertures of 50-cm to 1-m diameter, spectral filtering of ~ 0.1nm, and detector field of view (FOV) of < 200 μrad ($1/e^2$ diameter, set by the detector size and spatial filter), there is a clear difference between night and day regimes [3]. At night, polarization errors in the QC optics dominate over background, and so SNR can be improved by increasing the size of the receive aperture. In contrast, sky radiances are as much as a factor of 10^9 higher in daylight than at night, and background becomes the dominant error source: increasing the receive aperture will not improve the SNR in this case.

Achieving sufficient SNR for QKD in daylight as well as at night, which is desirable for high availability, is possible with a narrow beam-width, such as the 25-μrad ($1/e^2$ diameter) from a diffraction-limited 10-cm diameter aperture at 780 nm. However, Alice must point the quantum beam accurately at Bob, but typical satellite position and attitude knowledge uncertainties are such that open-loop pointing errors are comparable to the beam width. Similarly, the uncertainty in the ephemeris typically available to Bob will be larger than the FOV of his detectors. The problems of link acquisition and tracking can be overcome using uplink and downlink optical beacons at wavelengths outside the sensitive range of the single-photon detectors. Giving Bob's uplink beacon sufficient divergence so that it can be acquired by a position-sensitive detector within the space terminal, provides a pointing reference for the downlink quantum beam. Using a fast-steering mirror in the optical path, with closed-loop tracking of the reference direction reduces angular jitter of the quantum beam to a fraction of its width. Similarly, a

downlink beacon with sufficient divergence, co-boresighted with the quantum beam, can be detected by a position-sensitive detector in the ground terminal, allowing Bob to acquire and track Alice's quantum beam with a residual jitter much smaller than the FOV of Bob's photon detectors [5].

To achieve the low sifted key BERs required for QKD the QC receiver's polarization reference direction must be continuously aligned with the transmitter's to compensate for the field rotation introduced by two-axis telescope gimbals [5]. In 2006 we demonstrated over an outdoor range that by imparting a linear polarization to the downlink optical beacon, Bob can determine and apply the necessary compensation for field rotation rates of up to several degrees per second. In a 2004-2005 retro-reflector satellite experiment, and a subsequent ground experiment with simulated range variations of up to tens of ns per ms, we also demonstrated that imparting a known pseudo-random temporal sequence to the downlink beacon enables Bob to reliably synchronize his detected photon sequence with Alice's transmissions, in spite of typical range uncertainties. The optical beacons can also provide the conventional communications required for the QKD public channel, using only a small portion of the available optical bandwidth. In a recent laboratory experiment we have demonstrated real-time free-space QKD supporting AES encryption of four channels of streaming video (5 Mbps) over the downlink beacon, with key updates every few seconds. Also, we have devised a decoy-state BB84 protocol that is optimized for space-to-ground. The protocol reduces the number of conventional messages (to two in each direction), and their size (the largest is the uplink sifting message, amounting to no more than 100 bits for every secret bit produced), and has the computationally demanding tasks of decoy state channel estimation and error correction decoding located at Bob.

Satellite QC performance: We have analyzed the expected performance of our QC system concept over the full range of LEO orbital parameters, for a variety of ground sites, using a satellite-to-ground QC link model that incorporates orbital, atmospheric, turbulence, photon production and detection, decoy protocol, and acquisition, tracking and pointing factors. For illustration we will describe a hypothetical example of a QC terminal on the International Space Station (ISS, orbital altitude ~ 350-km, inclination 51.6°), with a hypothetical QC ground terminal in Los Alamos, NM, USA (~ 36° N latitude). With an orbital period of 91 minutes, the ISS is above the Los Alamos horizon ~ 4 times each day, for an average time of 4.5 minutes. This is a short time for establishing a QC link with a high enough SNR for QKD and completing a session with sufficient statistics to permit a precise security statement. Approximately 30% of all possible contacts culminate at elevations angles greater than 40° above the horizon. These contacts are both longer (~ 6 minutes average), with shore ranges and hence lower optical losses, and so provide better QKD opportunities than lower elevation contacts.

Taking an annual average over all possible night contacts shows that, at a 10MHz clock rate, ~ 10^5 secret bits would be possible per contact, using: a 10-cm diameter transmit aperture, with 3-μrad residual pointing bias and jitter; a 1-m diameter receiver, with 10-μrad residual pointing bias and jitter; a 10-s acquisition time; a three-level decoy protocol; a transverse coherence length of 5cm at 500nm at zenith; and a "high desert" atmospheric aerosol content. From a decade of National Weather Service data we determined that the annual average probability of a cloud-free-line of sight for our hypothetical ground location is 33%, indicating that we could expect to obtain this projected performance on ~ 210 of the night contact opportunities per year. (Additional secret bits could be produced under scattered cloud conditions; the annual probability of cloud-free or scattered clouds is ~ 70%.) We therefore project that night contacts alone could result in > 20Mbits of secret key per year to a single ground site.

Daylight QKD will be possible during contacts when the ISS is in regions of the sky with the lowest radiance, corresponding to solar scattering angles ~ 90°. For a given satellite-to-ground contact geometry there will therefore be both seasonal and time-of-day variation in the secret bit yield. Taking a representative 5-minute duration contact in which the ISS rises above the Los Alamos western horizon, culminates at 50° elevation in the north, and then drops below the eastern horizon, we find that daylight secret bit yields ~ 50kbits are possible under cloud-free conditions, using the same model parameters as for night contacts.

Conclusions: Using the architecture that we have developed, LEO satellite-to-ground QKD will be feasible with secret bit yields of several hundred 256-bit AES keys per contact. With multiple ground sites separated by ~ 100km, mitigation of cloudiness over any single ground site would be possible, potentially allowing multiple contact opportunities each day. The essential next step is an experimental QC-sat. A number of LEO-platforms would be suitable, ranging from a dedicated, three-axis stabilized small satellite, to a secondary experiment on an imaging satellite, to the ISS. With one or more QC-sats, low-latency quantum-secured communications could then be provided to ground-based users on a global scale. (Air-to-ground QC would also be possible.)

REFERENCES

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175.

[2] R. J. Hughes and J. E. Nordholt, *Physics World*, **May 1999**, 31 (1999); R. J. Hughes et al., *Lect. Notes Comp. Sci.* **1509**, 200 (1999).

[3] R. J. Hughes et al., *New J. Phys.* **4**, 43.1-43.14 (2002).

[4] See, for example, T. Schmitt-Manderbach et al., *Phys. Rev. Lett.* **98**, 010504 (2007).

[5] J. E. Nordholt et al., *Proc SPIE* **4635**, 116 (2002).

[6] J. G. Rarity et al., *New J. Phys.* **4**, 82.1 (2002); M. Aspelmeyer et al., *IEEE J. Sel. Top. Quan. Elect.* **9** 1541 (2003); C. Bonato et al., *New J Phys* **11**, 045017 (2009).

[7] M. Toyoshima et al., *Acta Astron* **63**, 179 (2008).

[8] M. Er-Long et al., *New J Phys* **7**, 215 (2005).

[9] J. W. Harrington et al., quantph/0503002v1 (2005).

[10] D. Rosenberg et al., *New J. Phys.* **11**, 045009 (2009).

[11] P. Rice and J. Harrington, quant-ph 0901.0013 (2009).

[12] W.-Y. Hwang, *Phys. Rev. Lett.* **91**, 057901 (2003); X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).