Ground to satellite secure key exchange using quantum cryptography

J G Rarity\textsuperscript{1}, P R Tapster\textsuperscript{1}, P M Gorman\textsuperscript{1} and P Knight\textsuperscript{2}
\textsuperscript{1} Optronics Department, QinetiQ, Malvern WR14 3PS, UK
\textsuperscript{2} Space Department, QinetiQ, Farnborough GU14 OLX, UK
E-mail: rarity@qinetiq.com

New Journal of Physics 4 (2002) 82.1–82.21 (http://www.njp.org/)
Received 26 June 2002, in final form 7 October 2002
Published 29 October 2002

Abstract. We examine the possibility of secure key exchange between a ground station and a low earth orbit satellite using the technique of quantum cryptography. The study suggests there are no technical obstacles to building a system that could exchange keys at kilobaud rates between a metre diameter telescope on the ground and a satellite with a 10 cm diameter lightweight telescope.

1. Introduction

With the exponential expansion of electronic commerce the need for global protection of data is paramount. Conventional key exchange methods generally utilize public key methods and rely on computational complexity as proof against tampering and eavesdropping. Satellite systems thus require future-proofing against the rapid improvements in computational power that may occur during their operational lifetime (many years). Here we discuss the feasibility of a satellite based key exchange system using free-space quantum cryptography (QC) [1]–[6]. Such a key exchange system could provide the highest security method for exchanging keys between any two points on the globe. The method of QC has its security based on the laws of nature and is, in principle, absolutely secure against any computational improvements.

This paper begins with an introduction to the QC technique (1.1) and a short review of the state of the art (1.2). We then introduce the satellite key exchange problem and suggest three possible apparatus arrangements (1.3). Section 2 attempts to define the key performance metrics on which we can assess particular system designs and sections 3–5 use these metrics to compare three different arrangements for satellite key exchange.

1.1. Introduction to quantum cryptography

A QC system uses single photon pulses and an encoding scheme based on either polarization or interference. In the polarization scheme [1] (figure 1) the sender (Alice) encodes a random binary
Figure 1. The principle of QC. Illustrated is the BB84 [1] protocol which utilizes weak polarized pulses. Security is guaranteed when the coding base is randomly switched between $0^\circ$ and $45^\circ$ using the polarization rotators. When Bob measures in a different base no information can be inferred (the pulse will randomly appear in either ‘0’ or ‘1’ detectors). Only when the same basis is used will the sent bit and received bit be the same.

bit string using vertically polarized pulses for 1 and a horizontally polarized pulse for 0. The receiver (Bob) then separates the two polarizations in a polarizing beamsplitter and incorporates a zero or one into his key, depending on which channel he detects the sent photon. Of course most sent pulses are lost in typical lossy transmission systems. However, the sender keeps a record of when the pulses were sent and the receiver uses a conventional (i.e. radio/telephone) link to tell him the time of arrival of received pulses. All un-received pulses are erased from the sender’s record, leaving identical random bit strings (keys) retained by the sender and receiver. A further subtlety guarantees the absolute security of the system. The sender randomly introduces a $45^\circ$ polarization rotation on the sent pulse and the receiver randomly introduces a $-45^\circ$ polarization rotation. Now the sent bit is randomized whenever only one rotator is present. The sender and receiver compare their records of the presence and absence of the rotator and retain only the received bits when either both rotated OR when both did not rotate the polarization. Again the result is that the sender and receiver end up with an identical random bit string which can be used as a key.

In a practical system these initial keys will not be identical but will differ in a small percentage of bits. This arises due to technical imperfections such as dark counts and apparatus defects. However, these errors are typically only a few per cent of key bits and can be corrected by simple secure hashing protocols [7] over the classical link between sender and receiver.

To intercept and gain information on the key an eavesdropper must make measurements on some or all of the sent pulses. An eavesdropper can intercept, measure and resend every pulse but has to guess the random basis. This results in a 25% error rate in the key established between
sender and receiver. The sender and receiver can monitor for eavesdropping by monitoring the
error rate of their system. Any increase of the error rate above a threshold value can be interpreted
as an insecure line. Below the threshold the natural error rate can be assumed to imply some
information leakage to the eavesdropper but absolute security can be regained by applying a
privacy amplification algorithm [8] (with suitable reduction of key length).

There are other interferometric coding schemes that can be used [9]–[11] but they
require temperature-stabilized interferometers at both sender and receiver. This would increase
complexity and payload weight without any clear advantages over the polarization coding in this
application.

1.2. State of the art

To date two groups have succeeded in exchanging keys over free-space ranges greater than
1 km [4]–[6] and ongoing experiments show that ranges of 10 [12] and 23 km [13] can easily
be reached. In all experiments the first steps are being taken to reduce the size, mass and power
consumption of the equipment primarily to allow portability in the short term and fully automated
remote operation in the long term.

Lightweight designs of transmitter and receiver are emerging [2, 13, 14]. These tend to be
based on combining or splitting the light in passive beamsplitters, thus avoiding active optical
elements. The generic system consisting of a four-laser transmitter (‘Alice’) and a four-detector
receiver (‘Bob’) is shown below (in figure 2). In Alice four near-identical diode lasers are
combined in beamsplitters. Each laser is rotated to input one of the four polarizations into the
system. The lasers are individually addressed from a switched short pulse driver. To ensure
that the lasers cannot be distinguished they pass through a narrow-band filter (F) and mode
filter (A) and are collimated by a lens (L). Further attenuation (At) is needed to bring the pulses
down to the single-photon level. In the generic receiver light collected in a telescope (L) is
split into two beams by a non-polarizing \(\frac{50}{50}\) beamsplitter. This beamsplitter acts as a passive
randomizing element directing the photons either to a \(\pm 45^\circ\) polarization measurement or to a
\(0/90^\circ\) polarization measurement. One of four photon-counting detectors will receive a count
and this uniquely determines the bit value and measurement basis. Being entirely passive this
system has no upper limit to laser repetition rates or sent bit rate. This rate is, however, limited
by the timing resolution (jitter) in the detectors. Surprisingly detector dead time does not affect
the system because received bit rates are low due to \(\sim 30–40\) dB of losses.

1.3. Key exchange to satellites

In this paper we set up the general scenario for a key upload system using QC. We compare and
contrast three possible methods for key exchange to satellites based on the QC technique. The
three options analysed are:

(A) Laser and encoding on the ground with detector on the satellite.
(B) Laser and encoding on the satellite with detector on the ground.
(C) Laser and detector on the ground, and a retro-reflector and polarizer on the satellite.

We conclude that all three systems could be used to exchange keys between a low earth orbit
satellite (800–1600 km range) and ground stations across the globe. At this time we limit
ourselves to night-time operation to avoid problems with background light. However, narrow-band filtering will probably allow daylight operation. The expected key exchange rates are up to 10 000 bits s⁻¹ and payloads could be as light as 2 kg. We emphasize that this is a feasibility study and not a design study and make no final conclusions about the choice or detailed design of the best system for a first experiment. We also note similar conclusions were reached in a parallel US-based study [15] on quantum key exchange while various classical communication schemes have actually been demonstrated in space experiments [16, 17].

However, at this stage we find that the highest bit rate and lowest launch mass could be obtained from option (B) based on the system described in this paper. This option involves some risk associated with controlling, in space, the temperature of four lasers to match their wavelengths to 0.1 nm and their pointing from the satellite to the ground with an accuracy of order 10 μR. A low risk option is (A) where the transmitter is ground based. Here there is a bit rate penalty because mass restrictions limit the satellite receiver optics to <30 cm and preferably ~10 cm diameter. This option also requires an active pointing system on the ground capable of counteracting the rapid beam wander due to turbulence in the earth’s atmosphere. The retro-reflection scheme (C) would be competitive if a suitable low-mass high-speed polarization modulator could be developed.
The ground to satellite scenario

The generic satellite system is shown schematically in figure 3. We list below the key elements and performance metrics of such a system:

**Ground telescope, tracking, pointing.** Typically we will be able to use a telescope on the ground with a diameter up to 1 m although a smaller portable system may be preferable in some circumstances. The ground telescope must be able to track the satellite and, in some cases, land a relatively small diameter beam (10 m) on the satellite.

**Turbulence.** Obviously all systems will be sensitive to atmospheric turbulence (the ‘seeing’). Typical turbulence wander at the top of the atmosphere will be of order 10 µR (daytime) if we choose a high altitude (desert/mountain top) ground station. Worse wander is expected at sea level (up to 100 µR). Thus upward pointing optics that has a field of view/beam spread of >100 µR will not be strongly affected by turbulence. Downward pointing optics will tend not to suffer from turbulence beam wander as the beam diameter at the top of the atmosphere will be greater than the beam spread due to passage through it. At this stage we have neglected lens and speckle effects of the turbulence.

**Satellite optics and pointing stability.** The satellite must be set to point roughly in the direction of the ground station for the duration of the pass. Here we assume 10 mR accuracy or 0.5° satellite alignment on the ground station.
Fine alignment can then be made with a tip-tilt mirror in the optical train. To ensure that the optical link is maintained we will require a minimum pointing accuracy from the optical system on the satellite. The satellite optics must look at the ground telescope to within this accuracy throughout the pass. We know from previous space optical communications experiments that pointing accuracies of <5 µR can be achieved from space [16, 17]. Here we assume the maximum deviation required is 0.5° but if the satellite is not pointing to 0.5° then a wide-angle (gimbal-mounted) alignment mirror is needed at the exit of the telescope, adding extra mass to our system.

**Satellite optics rotation stability.** If we are using a polarization encoding scheme then any relative rotation of the earth station and satellite around the axis of their connecting line will have to be compensated. Correction should be done at the ground station for simplicity.

**Satellite payload and power.** Both volume and mass of the satellite QC system will need to be minimized. For small satellites typical launch costs are >Euro100 000 kg⁻¹, warranting quite a lot of effort in weight reduction. In a classical optical communications experiment launched on STRV-2 a mass of 14 kg was achieved [16]. However, this included a full hemispherical field of view pointing gimbal and dual telescopes for full transceiver operation. Without the gimbal and with reduced complexity we expect to build systems with a total mass below 5 kg and have a target of below 3 kg. There is a similar requirement to minimize power consumption on board the satellite. Typically we expect a satellite power budget below 100 W when operational [16].

**The loss budget and satellite range.** We assume in this paper that the satellite would be in a polar orbit at an altitude of about 800 km. The satellite will have a period of about 90 min travelling at about 7.5 km s⁻¹. Not all passes will bring the satellite overhead: in fact, the earth rotates about 0.4 R per orbit and thus we expect the nearest night approach to be <0.2 R of earth rotation. For a ground station above 30 degrees latitude a worst case pass will then have a closest approach of 1580 km. To guarantee a nightly key exchange we need a system that operates out to >1600 km. On the other hand, when the satellite passes nearly overhead visibility to this range will allow measurements over >2700 km of the satellite path or a key exchange duration of 360 s. If the maximum range is only 1000 km then key exchange would be possible on less than half the nights. Daylight operation brings two passes daily and thus a lower range for daily operation.

Losses arise from diffraction spreading of the beams and wander of the beams due to atmospheric turbulence. Within this work we have assumed that atmospheric absorption losses are low, implying operation on a clear night (∼70% transmission, see below). We can lump together detector efficiency (70%), filtering (70%) and optical system transmission (60%) in an effective receiver efficiency of η ∼ 0.3 before we add diffraction and beam-wander losses (geometric losses). The divergence half-angle (1/e²) for Gaussian beams with 1/e² radius \( W_0 \) is given by

\[
\theta = \frac{\lambda}{\pi W_0}.
\]

In a standard collimating telescope the small diameter beam is de-focused by a negative lens and expands to fill the output lens which collimates hopefully to the diffraction limit. We can ensure
that 98% of our Gaussian beam passes through this lens of diameter $D$ when $2W_0 = 0.7D$. This sets our minimum divergence of our collimated beam as

$$2\theta = \frac{1.8\lambda}{D}.$$  \hspace{1cm} (2)

For instance the typical full divergence for a 100 mm lens illuminated by 650 nm light is thus $\sim 12 \mu R$. Within this $1/e^2$ angle we will collect 86% of the light (98% in 17 $\mu R$). However, if we intercept a large Gaussian beam diameter $2W$ with small diameter telescope $D_T$ we will collect a fraction

$$L_g = 1 - \exp\left[\frac{2D_T^2}{(2W)^2}\right] \approx \frac{D_T^2}{2W^2}$$  \hspace{1cm} (3)

of the light.

**Expected key exchange rate ($K$).** This will essentially be a product of the pulse repetition rate of the system $R$, the number of photons per pulse $M$ (typically $M < 0.1$), the atmospheric transmission $T$, geometric loss $L_g$, detection system lumped efficiency $\eta$ and the protocol efficiency (50%):

$$K = RMTL_g\eta/2.$$  \hspace{1cm} (4)

**Loss tolerance and error rates.** The system range is limited primarily by the background counting rate at the receiver which contributes to the bit-error rate. With a background count rate per second $B$ the gated background count probability per pulse per detector is

$$P_b = Bt$$  \hspace{1cm} (5)

where $t$ is a time gate set by the synchronization between transmitter and receiver. There are four detectors and half of the background pulses will lead to errors (the other half fortuitously match the sent bit). The background error rate is thus

$$E = 0.02 + \frac{2Bt}{MTL_g\eta}$$  \hspace{1cm} (6)

where we assume a 2% base error rate due to optical element imperfections. The error correction scheme is optimum for error rates $E < 0.07$, Thus we see that the minimum transmission is simply related to the background count rate

$$TL_g \geq \frac{40Bt}{M\eta}.$$  \hspace{1cm} (7)

Clearly the error rate is independent of the pulse repetition rate but highly dependent on the gating. Present systems achieve around 1 ns synchronization and at night with 10 nm bandwidth filters the background can be reduced to $B < 100$ counts/s/detector [6, 12]. Putting these values into equation (6) with $\eta \sim 0.3$ gives us a limit on the detected photon rate

$$TL_gM \geq 1.3 \times 10^{-5}/\text{pulse}$$  \hspace{1cm} (8)

and if we accept that security is guaranteed by $M \sim 0.1$ then the system can tolerate about 40 dB loss. Such low background rates are only possible during night operation. If sub-nanometre wide filters can be used daylight operation may become possible.
Security. Each system will have some susceptibility to eavesdropping in various cunning ways. These routes to eavesdropping will have to be protected against. One common problem with the faint pulse system used here is the susceptibility to eavesdropping on multi-photon pulses. This involves an eavesdropper hijacking the weak pulse beam at the exit of the transmitter, selecting only those pulses with more than one photon and measuring in such a way as to get partial information on the key. The eavesdropper can then can re-inject pulses at the receiver, thus bypassing the channel transmission losses. To avoid this possibility requires that $M$ reflect the sophistication of the potential eavesdropper. An extreme technology projection assumes the eavesdropper can sense and split two-photon pulses while blocking one-photon pulses, store one photon (until measurement bases are revealed) and send the other to the receiver without seeing any loss. This scenario can be guarded against by limiting $M \leq TL_g$ \cite{18, 19}, suggesting that a system operating at $M \leq 0.1$ can tolerate only 10 dB of transmission loss. Technologies for non-linear splitting of pair photon pulses and storage of single photons for many seconds (or hours if bases are kept secret until needed) are decades away at present. With present technologies the eavesdropper is limited to a strategy where the coding basis and bit value are uniquely determined from three-photon detection events in a standard receiver \cite{6}. To do this without discovery the rate of three-photon detection at the eavesdropper must be greater than the normal rate of detection of single photons at the receiver. This implies that setting $M^2 \leq 24TL_0$ is an adequate security level to guard against this attack. A system operating at $M \leq 0.1$ is secure against attack up to 34 dB of loss.

It is probably more realistic to protect against intercept–resend eavesdropping, as discussed above, using passive and active monitoring of the viability of the free-space channel. By definition the entire free-space channel is visible during the key exchange and any eavesdropper must remain invisible to all wavelengths of the electromagnetic spectrum that can be used to monitor security. In this case the limit to the number of photons per pulse is less restrictive and $M \leq 0.4$ may still allow secure key exchange (see \cite{12, 15}).

In the system described in figure 2 there is always the possibility that the different lasers are distinguishable. To prevent this a single mode aperture and narrow-band filter ($<1$ nm) are used to ensure the lasers have the same spectral and spatial characteristics. Diode laser emission wavelengths drift by about 0.12 nm °C$^{-1}$, thus loose temperature control to 1° is required. If ultra-narrow-band filters ($\sim 0.1$ nm) are used to allow daylight operation then careful temperature control is required ($<0.2°$). Doppler shifts from the motion of the satellite set the minimum filter bandwidth to $\sim 5 \times 10^{-5}$ of a wavelength. Diode lasers producing pulses around 100 ps long are not time-bandwidth-limited but are somewhat chirped. This suggests methods of discrimination based on timing to better than 100 ps to discriminate the different chirps. This can be guarded against by adding an electronic jitter of $\sim 100$ ps to effectively randomize the pulse and chirp timings.

Time synchronization. To allow a short gate time to be used the timing at each end should be synchronized to better than 1 ns. Two approaches to this are being considered. The first is to use the arrival times of the photons (key bits) to drive a software phase locked loop \cite{6} and the second relies on a periodic bright pulse, of a different wavelength, to lock the timing \cite{4}. The former requires a key rate of a few hundred per second to allow timing adjustment every 100 ms. The latter could be implemented with a bright pulse repetition rate comparable to the dim pulse repetition rate but requires careful matching of two beams widely separated in wavelength. Again, varying Doppler shifts due to the satellite motion ±3–5 km s$^{-1}$ will slowly change the
repetition frequency but can be tracked and corrected for.

**Wavelength.** The choice of wavelength is set by the atmospheric transmission and the detector sensitivity. Throughout the visible region the atmosphere is, of course, highly transmissive (>60%) although wavelengths shorter than 600 nm are increasingly attenuated due to aerosol and molecular Rayleigh scattering. Beyond 1050 nm the water absorption effects begin to be strong and in the NIR various absorption features due to water and oxygen reduce transmission. Windows of high transmission occur at

- 650–670 nm $\sim$ 65%
- 740–750 nm $\sim$ 70%
- 770–775 nm $\sim$ 72%
- 850–880 nm $\sim$ 74%
- 1000–1060 nm $\sim$ 75%.

Beyond 900 nm silicon detectors rapidly lose efficiency. The 650 nm region is close to the highest efficiency detection region (70%) although detection efficiencies as high as 40% can be achieved out to 850 nm. Systems operating in the 600, 700 and 800 nm bands have now been demonstrated [4, 6, 12]. Detailed curves showing the various contributions to atmospheric absorption are seen at [20]. In the following we assume a wavelength in the 650 nm region because the diffraction spread is smallest. Other work suggests that the 770 nm band gives the highest overall bit rates [15].

**Classical channel.** Common to all systems is the classical channel which must be capable of exchanging digital data at high bit rates to allow interactive alignment, time synchronization, key sifting and error correction to be carried out in real time. Ethernet bandwidths (10 MHz) are needed for real-time operation. Lower classical bandwidth would require some time after optical key exchange for the protocol to be completed, thus limiting the number of key bits that could be exchanged on a typical pass.

In the following we use these metrics to compare and contrast the three approaches.

### 3. Laser and encoding on the ground with detector on the satellite

Ostensibly this is the simplest system although the ground-based pointing stability requirement is high and the loss budget due to diffraction spreading is large. A typical system is illustrated in figure 4.

**Ground telescope, tracking, pointing and turbulence.** Typically one would use a ground laser expanded to a near-diffraction-limited 30 cm beam. This would imply $\sim$4 $\mu$R diffraction spread. To keep such a small spot pointing at the satellite requires a high-speed (<50 ms response time) active pointing scheme correcting for turbulence wander at the ground station. On the satellite the pointing and tracking requirement would be less stringent (100 $\mu$R) but both the ground station and the satellite would need to be fitted with laser beacons (guidestars). A suitable point-ahead scheme will be needed as the satellite velocity will take it a considerable distance (tens of metres or 20–50 $\mu$R) in the time it takes a beacon to reach the ground and a signal to return. This also
Figure 4. (a) Satellite station receiver. This includes a lightweight receiver module, guidestar laser for ground tracking and CCD camera to maintain closed loop pointing. An on-board lightweight processor handles the pointing and tracking, time synchronization and key management. Key sifting and error correction is carried out via a microwave link. (b) The ground station incorporates the compact four-laser transmitter with a high power ‘guidestar’ laser and pointing and tracking CCD. The closed loop tracking and pointing system will need to maintain pointing to better than 4 µR.
means that the guidestar beam will not pass through the same column of atmosphere as the up-going signal beam. As most turbulence occurs in the 1 km boundary layer where beam deviation will be at most 50 mm (in a 30 cm wide beam) we expect this will not strongly affect the closed loop pointing. The best space based optical communication experiments are just achieving 2 $\mu$R tracking without turbulence [17] and we suspect that from the ground one might achieve 3–5 $\mu$R tracking accuracy. This will degrade our effective beam spread to around 6 $\mu$R.

**Satellite optics pointing stability.** We require only that the ground station remain within the field of view of the detectors. The angular field of view $\theta_o$ at the output optic is given by

$$\theta_o = \frac{D_d}{f}$$

where $D_d$ is the detector diameter (typically 500 $\mu$m) and $f$ is the telescope focal length. For a 10 cm (30 cm) optic $f/10$ telescope the field of view is 0.5 mR (0.17 mR). Tracking accuracy at the satellite is thus not as stringent ($>100$ $\mu$R). With such a wide field of view operation in daylight conditions may be impossible due to excess background light. Reducing the detector field of view and pointing to better than 100 $\mu$R may be preferred. When the field of view is less than 100 $\mu$R pointing ahead of the image of the ground based guidestar becomes important.

**Satellite optics rotation stability.** The effective orientation of the satellite would be monitored by measuring guidestar polarization at the ground station and correcting at the ground.

**Satellite payload and power.** With 10 cm optics the target of 3 kg may be reached but 30 cm optics will be difficult to build below 5 kg. Total package power dissipation of <100 W is easily achieved. This includes 4 A at 5 V for detectors (including high voltage supply and Peltier cooling), 4 W computing, 10 W interfaces, plus 6 W point and track system.

**Loss budget and maximum range.** We assume $\sim 6$ $\mu$R combined pointing and diffraction loss for 30 cm ground optics. At 1000 km range loss $TL_g = 0.00036$ ($\sim 34$ dB) for 10 cm satellite optics and $TL_g = 0.0032$ ($\sim 25$ dB) for 30 cm diameter satellite optics, assuming atmospheric transmission $T \sim 0.65$. Setting the maximum loss tolerance at 35 dB (for security and error correction reasons, see section 2), the maximum range is just 1100 km with 10 cm satellite optics and >3000 km with 30 cm optics.

**Expected key rates.** Assuming a laser repetition rate of $R = 100$ MHz and $M = 0.1$ photon per bit in equation (4) we obtain $K \sim 4500$ bits $s^{-1}$ at 1000 km and $K \sim 1000$ bits $s^{-1}$ at 2000 km. For 10 cm satellite optics this becomes $K \sim 450$ bits $s^{-1}$ at 1000 km (maximum range is about 1100 km).

**Error rates and loss tolerance.** Background light errors could be a problem when transmitting from populated areas. However, limiting ourselves to 35 dB maximum loss at maximum range implies a maximum background $B < 240$ counts $s^{-1}$ (equation (7)) which is easily achieved at night with nanometre bandwidth filters.

**Security.** The system would be highly secure when using BB84 protocol as long as care was taken to make all lasers indistinguishable as described in section 2.
4. Laser and encoding on the satellite with detector on the ground

The satellite optics is shown in figure 5(a). The four-laser source can be made extremely compact and lightweight. A beamsplitter picks off a view of the ground for a CCD camera so that closed loop pointing control can be effected. The beam is then expanded to 10 cm to send to the ground. With an f/6.5 10 cm aperture telescope a 1.2 cm CCD will have a field of view of 18 mR or $\sim 1^\circ$. To bring the ground station guidestar into view thus requires a satellite pointing capability better than $1^\circ$. With a 1000 pixel camera each pixel covers 18 $\mu$R. For closed loop pointing we envisage using a small (rapid read-out) window of interest on the camera. Intensity interpolation should allow location of the guidestar to better than 5 $\mu$R, thus allowing pointing to this order of accuracy. This is much less than the 12 $\mu$R diffraction limit of our telescope.

The receiver (figure 5(b)) is in the ground station with a fixed telescope with up to a 1 m diameter. It too has closed loop tracking but with lower resolution than the transmitter.

*Ground telescope, tracking and pointing.* To make it easy to track the satellite a field of view $> 100$ $\mu$R could be engineered. This would require an effective $f/5$ 1 m telescope with 0.5 mm detectors. Using high numerical aperture relay lenses before the detectors we could reach an effective $f/2$ telescope (250 $\mu$R field of view). In this form daylight background levels will be high and night operation will be preferred. With a large field of view, point-ahead tracking corrections may not be necessary.

*Turbulence.* As this is a downward pointing system we expect very little wander of the beam compared to its 12 m diameter footprint. The detector within the ground system will have to have an effective field of view greater than 10 $\mu$R to avoid wander of the image (see above). Small scale turbulence ($< 1$ m) could still cause weak lens and speckle effects. Satellite vibrations and drift would still need to be corrected for.

*Satellite optics pointing stability.* With the laser on the satellite we will have to point with an accuracy of 12 $\mu$R. This will require the use of an upward pointing beacon laser co-aligned with the ground telescope. The bandwidth of this system should not be high, involving probably drift timescales of the order of seconds. Thus we could use a slow tip-tilt mirror at an intermediate stage. Placing a tip-tilt mirror at a position where beam diameter is $\sim 25$ mm, the $\pm 0.5^\circ$ stability of the satellite is magnified by a factor of 4. The tip-tilt system thus requires a full-scale tilt of order 34 mR ($\pm 2^\circ$) and the closed loop needs to operate with an accuracy $< 40$ $\mu$R.

*Satellite optics rotation stability.* The effective orientation of the satellite would be monitored by measuring polarization at the ground station and corrected at the ground.

*Satellite payload and power.* With 10 cm optics the target of 3 kg may be reached. Total package power dissipation of $< 100$ W is expected.

*Loss budget and maximum range.* With 10 cm optics the diffraction spread of a 650 nm beam is of order 12 $\mu$R and the ground footprint would be 12 m from 1000 km. This gives a loss in a 1 m diameter telescope at the ground station of $T_{L_g} = 0.0046$ ($\sim 23.5$ dB). With a 0.5 m diameter telescope $T_{L_g} = 0.0012$ ($\sim 29.3$ dB). With 35 dB maximum tolerable loss the maximum ranges...
Figure 5. (a) Satellite based transmitter. This includes a lightweight laser system using matched lasers and electronic switching between them to select the four polarizations used in the BB84 protocol. Pointing and tracking is controlled to the ±0.5° level by the satellite while a closed loop system incorporating CCD tracking electronics and a tip-tilt mirror controls fine pointing to better than 10 µR. (b) Ground station with telescope and boresighted beacon laser. The four-detector receiver design provides a wide field of view (100 µR at the telescope output).
are >4000 km for a 1 m telescope and >2000 km for the 0.5 m telescope. At these higher ranges we have had to take account of the extra loss from atmospheric transmission at low elevation angles in the atmosphere.

**Expected key rate (at 1000 km range).** The key rate will be limited by the maximum repetition rate of the lasers and the loss. Using equation (4) \( R = 100 \, \text{MHz} \) and \( T L_g = 0.0045 \) we expect a ground key rate at 0.1 photon per bit of \( K \sim 6600 \, \text{bits s}^{-1} \). For a smaller \( \frac{1}{2} \) m ground telescope \( K \sim 1600 \, \text{bits s}^{-1} \).

**Error rate.** As we are looking up (at a night sky) the error rates due to background light will be low. Again, using a maximum loss of 35 dB in equation (7) implies a maximum background \( B < 240 \, \text{counts s}^{-1} \). With suitable filters this may allow operation at night when the satellite is still in sunlight. However, daylight operation is not possible due to the wide viewing angle (100 \( \mu R \)) proposed for ease of tracking in the receiver. Better tracking might allow a smaller field of view and thus limit daylight background.

**Security.** The system would be highly secure when using BB84 protocol. The control of the wavelength of the four lasers to within 0.1 nm is also required. Any difference in wavelength could be used to discriminate between bit values.

5. Laser and detector on the ground, and a retro-reflector and polarization modulation on the satellite

Here the system comprises a pulsed laser system at ground level boresighted with the tracking telescope that acts as a receiver (Bob). This laser sends a relatively broad beam up to the satellite. On the satellite there is retro-reflector formed by a simple telescope with a mirror set at its focal point. Before the mirror is a polarization modulator which can encode the required four polarization states onto the retro-reflected beam.

**Ground telescope, tracking and pointing.** This system can use a relatively high divergence ground based laser beam (say 100 \( \mu R \)) and thus only requires that the ground telescope points with 100 \( \mu R \) accuracy at the satellite (this is much greater than the turbulence wander and larger than point-ahead corrections). The return beam will, however, deviate somewhat from true retro-reflection essentially due to the Doppler effect occurring because of the satellite velocity \( V \sim 7 \, \text{km s}^{-1} \) relative to the velocity of the earth’s surface. The deviation angle is of order \( \theta = 2V/c \), corresponding to some 47 \( \mu R \) of deviation (47 m at the earth’s surface for a satellite height of some 1000 km). At first sight this system is then unworkable as this is much larger than the diffraction spreading (\( \sim 12 \mu R \)) and we would require separate tracking for the laser and telescope separated by varying distances, dependent on range. This can be solved by fitting a biprism element in the satellite optics as shown in figure 6. The biprism angle is chosen such that the passage through either side will divert the beam by exactly half the Doppler angle. A light beam entering the retro-reflection system will pass through the opposite side of the biprism on its return, thus suffering a deviation equalling the Doppler angle \( \pm \theta \). We will then obtain two return beams, one exactly co-linear with the incoming beam and the other deviated by \( +2\theta \). A more detailed analysis shows that, with a typical satellite, this correction scheme will return
Figure 6. (a) Satellite station using a polarization modulating retro-reflector. Doppler shifts due to the relative motion between satellite and ground are compensated by a biprism design. The CCD is used to point the satellite at the ground station with an accuracy set by the field of view of the retro-reflector ($>100\mu R$). A guidestar laser is used to lock the ground station pointing. (b) Ground station for the retro-reflection system. A bright pulsed laser is roughly collimated to point at the satellite. The guidestar/satellite image in the CCD camera is used for closed loop tracking to within the field of view of the receiver module ($100\mu R$).
the light to the ground station within its diffraction spread for most elevations above $50^\circ$. The biprism will effectively halve the returned light.

As the output from the retro-system is $\sim 0.1$ photons/bit this requires us to have at least 10 photons/pulse arriving in the 10 cm aperture of the satellite optics. The footprint of a 100 $\mu$R beam at the satellite is of order 100 m, implying $10^{-6}$ of the laser power will enter the satellite optics. For a system operating at 100 MHz repetition this implies $10^{15}$ photons s$^{-1}$. This implies a ground laser emitting around 3 mW of power in 100–200 ps pulses at 100 MHz. Power variation with range (and visibility) can be monitored by the satellite based single-photon detector (SPD).

**Turbulence.** With the biprism the return beam would pass through the same turbulence as the outgoing beam and this would correct for all wavefront tilt induced beam-wander. However small scale turbulence ($<1$ m) could still cause weak lens effects.

**Satellite optics pointing stability.** In the retro-reflection system we require only that the ground station remains within the field of view of the retro-reflector. This will usually be limited by the polarization switch which will have a limited acceptance angle. Present low voltage (200 V) electro-optic switches have a 10 mR field of view in a 1 mm beam, translating to 100 $\mu$R in an output beam of 10 cm diameter. However, a larger area liquid crystal device will offer a much wider field of view, up to 20 mR at the telescope entrance, which may only require pointing of the satellite to an accuracy of a degree. Tracking the ground station is achieved by locking the image of the ground station laser to the centre of a sensitive CCD camera.

**Satellite optics rotation stability.** The effective orientation of the biprism would have to be maintained normal to the satellite motion. This requires an accuracy of a few degrees. This effect could *not* be corrected from the ground.

**Satellite payload and power.** This is the key technological problem for this system. We assume again that a computing, 10 cm telescope and pointing system could be built to weigh less than 5 kg. The system could be made lightweight if a low voltage (10 V) polarization modulator could be found but present (multimode) electro-optic modulators require of the order of 200 V and thus the power supply could weigh $>9$ kg (assuming 8 MHz BW Gsanger Model Liv 8). We could use single-mode waveguide modulators and thus achieve low voltage modulation but then require accurate pointing (10 $\mu$R) of the satellite. Low voltage liquid crystal modulators are under development but can only reach 500 kHz operation at present while higher speed electro-absorption modulators do not yet have enough contrast [21]. Total package power dissipation of $<100$ W is expected with a low voltage system but will not be possible if bulk E-O modulators are used.

**The loss budget and maximum range.** The retro-reflected beam will be diffraction limited when the mirror is at the exact optical focus. For 10 cm optics this would mean a diffraction spread of $\sim 12$ $\mu$R and a 12 m spot on the ground. An extra 50% loss is also inherent in the biprism system. This gives a loss of $0.5TL_g = 0.0023 (\sim 26.5$ dB) in a 1 m diameter telescope and $0.5TL_g = 0.0006 (\sim 32$ dB) with a 0.5 m diameter telescope at the ground station. With 35 dB maximum loss the maximum ranges are $>3000$ km for a 1 m telescope and $>1800$ km for the
0.5 m telescope. The extra loss due to the biprism reduces the maximum range from the previous down-looking example.

**Expected key rate (at 1000 km).** The key rate will be limited by the maximum rate of modulation of the retro-reflecting polarization modulator. Using present technologies this is about $R \sim 10 \text{ MHz}$ in a 10 kg electro-optic system, $R = 0.5 \text{ MHz}$ in a 0.2 kg liquid crystal modulator. From the above $0.5T/L_g = 0.0023$ and $K \sim 330 \text{ bits s}^{-1}$ with $R = 10 \text{ MHz}$ and $K \sim 16 \text{ bits s}^{-1}$ with $R = 0.5 \text{ MHz}$. If a future lightweight modulator operating at 100 MHz is produced, bit rates of $K = 3300 \text{ bits s}^{-1}$ can be expected.

**Error rate.** Again equation (7) tells us that background counting rates below 240 counts s$^{-1}$ are fine, independent of repetition rate.

**Security.** The retro-reflection strategy will always be subject to the possibility of an eavesdropper looking into the satellite retro-system with a strong laser to measure the polarization rotation induced by the electro-optic modulator. To avoid this eventuality we monitor the incoming pulses with a sensitive SPD. 90% of the incoming laser light is directed to the SPD and the tracking CCD and only 10% passes to the retro-reflection system. This then provides a minimum $100 \times$ attenuation of light traversing the retro-system. Extra light injected by an eavesdropper to measure the polarization modulation for each pulse would be detected in the monitor SPD. The monitor SPD would also provide a time synchronization signal for the satellite circuitry from the timing of the arriving laser pulses.

### 6. Conclusions and future

We conclude that all three systems could be used to exchange keys between a low earth orbit satellite (800 km) and ground stations across the globe at least once every night. Key exchange rates of several kilobits per second can be expected when the satellite is at its closest approach to the ground station. Payloads of a few kg and tens of watts power consumption should be possible. With such a system we might expect megabits of key to be uploaded in a single pass (satellite in range for $\sim 100$–200 s). However, we have restricted ourselves to operation in the dark (background count rates less than 250 s$^{-1}$) as we suspect daytime operation will lead to error rates that are far too high. With this low background a 35 dB loss can be tolerated (see equation (7)). Higher losses can be tolerated if we improve synchronization to better than 1 ns or reduce the background further. We have assumed that intercept–resend strategies can be used by the eavesdropper. This is possibly a restrictive scenario in free space where the optical channel can be monitored at all times. Assuming eavesdropping only on light which is not detected at Bob allows a higher mean photon number to be used with consequently higher bit rates and higher loss tolerance.

At this stage we favour option (B), using a down-looking transmitter. Here the expected key rates are up to 7 kbits s$^{-1}$ when operating at 100 MHz repetition rates, $<1000$ km range and using a 1 m diameter telescope. The low loss of 24 dB should provide high immunity to background counts. The four-laser scheme in the transmitter could be engineered to be reliable, compact and lightweight. Various ways of ensuring that the laser wavelengths are indistinguishable are available, the simplest being through variation of laser current and operating...
Table 1. Summary table comparing performance of the three systems.

| Performance metrics | Laser on ground up to satellite | Laser on satellite receiver on ground | Laser on ground retro on satellite |
|---------------------|--------------------------------|--------------------------------------|-----------------------------------|
| Ground telescope    | 30 cm                          | (a) 1 m or (b) 0.5 m                 | (a) 1 m or (b) 0.5 m              |
| Ground tracking and pointing | 4 \( \mu \text{R} \) diffraction | >100 \( \mu \text{R} \) | >100 \( \mu \text{R} \) Detector limited |
| Turbulence          | Requires active turbulence correction to <6 \( \mu \text{R} \) | Passive system | Passive system |
| Satellite optics diameter | (a) 30 cm and (b) 10 cm | 10 cm | 10 cm |
| Satellite optics pointing ability | 100 \( \mu \text{R} \) Locked to ground laser guidestar | 12 \( \mu \text{R} \) Locked to ground laser guidestar | 100 \( \mu \text{R} \) Locked to ground laser guidestar |
| Satellite optics yaw stability | Corrected from ground | Corrected from ground | Corrected from ground |
| Satellite payload   | (a) >5 kg and (b) <5 kg | (a) and (b) <5 kg | (c) L-C modulator <5 kg, \( R = 0.5 \text{ MHz} \) (d) E-O mod 11 kg, \( R = 10 \text{ MHz} \) (e) Future mod <5 kg, \( R = 100 \text{ MHz} \) |
| Satellite power requirement | <100 W | <100 W | (c) <100 W (d) >300 W (e) <100 W |
| Maximum range for key exchange (34 dB loss) | (a) 1060 km and (b) 3000 km | (a) 4000 km and (b) 2000 km | (a) 3300 km and (b) 1800 km |
| The loss budget (\( TL_0 \)) at 1000 km | (a) 25 dB and (b) 34 dB | (a) 24 dB and (b) 29 dB | (a) 27 dB and (b) 32 dB |
Table 1. (Continued.)

| Performance metrics | Laser on ground up to satellite | Laser on satellite receiver on ground | Laser on ground retro on satellite |
|---------------------|---------------------------------|---------------------------------------|-----------------------------------|
| Expected key exchange rate at 1000 km<sup>a</sup> | (a) >100 00 bps (b) >1000 bps | (a) 6000 bps (b) 1500 bps | (c) 16 bps (d) 330 bps (e) 3300 bps |
| Error rates | 2–7% | 2–7% | 2–7% |
| Security | Good for 0.1 photon/bit | Good for 0.1 photon/bit | Good if anti-eavesdrop detector incorporated |
| RF link data exchange | 10 MB s<sup>−1</sup> preferable | 10 MB s<sup>−1</sup> preferable | 10 MB s<sup>−1</sup> preferable |
| Synchronization of clocks | Occasional bright pulses and PLL | Occasional bright pulses and PLL | Satellite anti-eavesdrop SPD used with PLL |
| Temperature stability required for satellite components | Detectors need cooling to −30 °C with stability 0.1 °C | Laser controlled to ±0.5 °C | E-O modulator needs ±2 °C |
| Key risks | Active point and track to <4 µR | Laser matching to 0.1 nm wavelength | Modulator technology |

<sup>a</sup> Note the key exchange rate quoted is for the raw key. Net key rates after error correction and privacy amplification would be between 10 and 50% of this value, depending on the actual error rate encountered [6, 15].

Temperature. Our preferred option is to select lasers that operate at the same wavelength and the same temperature and to mount all laser chips on the same heat sink and temperature control system. The lasers can also be passed through a narrow-band (<1 nm) filter at the transmitter to improve indistinguishability. The development of this space-qualified laser system is one of the key risks to realizing this design. Another key risk is the tracking of the ground station from the satellite with an accuracy better than 10 µR.

Options (A) and (C) are not yet ruled out. If active tracking and turbulence correction from ground to space achieves micro-radian accuracy with easily adaptable technology then option A proves to be low risk. Here there is a bit rate penalty because mass restrictions limit the satellite receiver optics to <30 cm and preferably ∼10 cm diameter. In this latter case the maximum range (1060 km) may only allow key exchange on favourable passes, limiting operation to <50% of nights. Option (C) becomes competitive if a lightweight, high-speed wide-angle polarization...
modulator becomes available, possibly from improvement of electro-absorption modulators [21]. This option also requires an active pointing system on the ground capable of counteracting the rapid beam-wander due to turbulence in the earth’s atmosphere.

In this paper we have made various simplifications mainly to make comparative evaluations of the three systems. In particular the bit rate will vary as a function of range and elevation of the satellite above the horizon and also in varying atmospheric conditions. Similarly error correction and privacy amplification will reduce effective bit rates by factors ranging from 2 to 10. Estimates of key exchange rates are thus order of magnitude calculations only. In a later paper we expect to study system B in more detail and estimate performance under various conditions using more sophisticated models of satellite orbit, atmospheric attenuation and security enhancement.

Finally we can propose a satellite based global key exchange system for key exchange between any two arbitrary points on the globe. This system would work by first exchanging keys between one ground station and the satellite. The satellite would then have to store the key securely until the second ground station came into view (up to several hours later). Exchanging the key with this second ground station would allow the first key to be sent down using an absolutely secure one-time-pad encoding scheme. The global reach of the system may be what drives the development but it will probably cost well in excess of ten million Euros (dollars) to build and fly.

Acknowledgments

K Wallace and R Blott of QinetiQ Space Department have provided various details on satellite operation.

References

[1] Bennett C H et al 1992 Experimental quantum cryptography J. Cryptol. 5 3–28
[2] Rarity J G, Owens P C M and Tapster P R 1994 Quantum random number generation and key sharing J. Mod Opt. 41 2435–44
[3] Buttler W T et al 1998 Practical free-space quantum key distribution over 1 km Phys. Rev. Lett. 81 3283
[4] Buttler W T, Hughes R J, Lamoureux S K, Morgan G L, Nordholt J E and Peterson C G 2000 Daylight quantum key distribution over 1.6 km Phys. Rev. Lett. 84 5652–5
[5] Rarity J G, Gorman P M and Tapster P R 2001 Secure key exchange over a 1.9 km free-space range using quantum cryptography Electron. Lett. 37 512
[6] Rarity J G, Gorman P M and Tapster P R 2001 Secure free-space key exchange to 1.9 km and beyond J. Mod. Opt. 48 1887
[7] Bennett C H, Brassard G and Robert J-M 1988 Privacy amplification by public discussion SIAM J. Comput. 17 210–29
[8] Brassard G and Salvail L 1994 Secret key reconciliation by public discussion, adventures in cryptography EUROCRYPT93 (Lecture Notes in Computer Science vol 765) (New York: Springer) pp 410–23
[9] Townsend P D, Rarity J G and Tapster P R 1992 Single photon interference in a 10 km long optical fibre interferometer Electron. Lett. 29 634–5
[10] Muller A, Breguet J and Gisin N 1993 Experimental demonstration of quantum cryptography using polarised photons in optical fibre over more than 1 km Europhys. Lett. 23 383–8
[11] Marand C and Townsend P D 1995 Quantum key distribution over distances as long as 30 km Electron. Lett. 20 1695–97

New Journal of Physics 4 (2002) 82.1–82.21 (http://www.njp.org/)
Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 Practical free-space quantum key distribution over 10 km in daylight and at night New J. Phys. 4 43

Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P, Tapster P R and Rarity J G 2002 Quantum cryptography: a step towards global key distribution Nature 419 450

Kurtsiefer C et al in preparation

Nordholt J E, Hughes R J, Morgan G L, Peterson C G and Wipf C C 2002 Present and future free-space quantum key distribution Proc. SPIE 4635 117

Korevaar E, Schuster J, Adhikari P, Hakakha H, Ruigrok R, Steiger R, Fletcher L and Riley B 1997 Description of STRV-2 lasercom flight hardware SPIE 2990 38–49

Tolker-Nielsen T and Oppenhauser G 2002 In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4, SILEX SPIE 4635 30

for general description see: http://spot4.cnes.fr/spot4_gb/pastel

Lutkenhaus N 1998 Security against individual attacks for realistic quantum key distribution Phys. Rev. A 61 052304

Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography Phys. Rev. Lett. 85 1330–3

http://www.soc.soton.ac.uk/RSADU/Icarus.html

http://mrr.nrl.navy.mil/overview.html