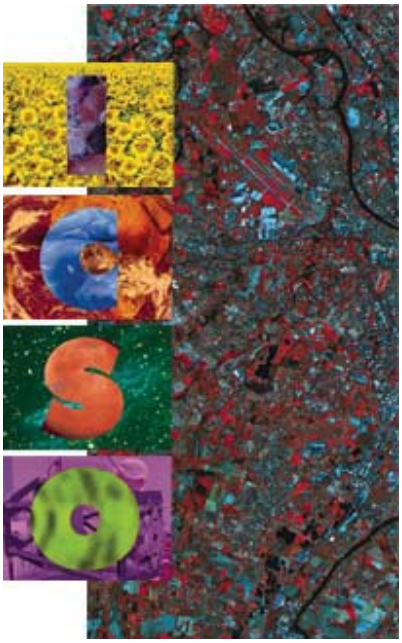
International Conference on Space Optics—ICSO 2000

Toulouse Labège, France

5–7 December 2000

Edited by George Otrio



Quantum cryptography to satellites for global secure key distribution

John G. Rarity, Philip M. Gorman, Paul Knight, Kotska Wallace, et al.

International Conference on Space Optics — ICSO 2000, edited by George Otrio, Proc. of SPIE Vol. 10569
105690W · © 2000 ESA and CNES · CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2307891

QUANTUM CRYPTOGRAPHY TO SATELLITES FOR GLOBAL SECURE KEY DISTRIBUTION

John G. Rarity[1], Phil M. Gorman[1], Paul Knight[2], Kotska Wallace[2] and Paul R. Tapster[1]

[1]DERA Sensors & Electronics, St. Andrews Road, Malvern, Worcs., UK.
[2]DERA Space, Farnborough, Hants., UK.

ABSTRACT *- We have designed and built a free space secure key exchange system using weak laser pulses with polarisation modulation by acousto-optic switching. We have used this system to exchange keys over a 1.2km ground range with absolute security. Building from this initial result we analyse the feasibility of exchanging keys to a low earth orbit satellite.*

1. INTRODUCTION

With the exponential expansion of electronic commerce the need for global protection of data is paramount. Conventional key exchange methods generally utilise 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 quantum cryptography [1-4]. Such a key exchange system could provide the highest security method for exchanging keys between any two points on the globe. The method of quantum cryptography has a security based on the laws of nature and is, in principle, absolutely secure against any computational improvements.

We have built a breadboard quantum cryptography system, which already can exchange keys out to 2km range (ground to ground). By refining this system we expect to reach tens of kilometres range. At present the system range is largely limited by turbulence induced beam wander in ground to ground optical paths. Based on the lower estimates of turbulence wander obtained in the vertical direction we expect to be able to reach 1000km suitable for key exchange to low-earth-orbit satellites. In this paper we introduce a possible optical arrangement and estimate its performance.

2. INTRODUCTION TO QUANTUM CRYPTOGRAPHY

A quantum cryptography (QC) system uses single photon pulses and an encoding scheme based on either polarisation or interference. In the polarisation scheme [1] (fig. 1) the sender (Alice) encodes a random binary number using vertically polarised pulses for 1 and a horizontally polarised pulse for 0. The receiver (Bob) then separates the two polarisations in a polarising 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 (ie telephone or radio) link to tell him the **time of arrival** of received pulses. All unreceived pulses are erased from the sender's record and identical random keys are retained by sender and receiver. A further subtlety guarantees the absolute security of the system. The sender randomly introduces a 45° polarisation rotation on the sent pulse and the receiver randomly introduces a -45° polarisation rotation. Now the sent bit is randomised whenever only one rotator is present. The sender and receiver compare their records of presence and

absence of the rotator and retain only the received bits when both rotated OR both did not rotate the polarisation. Again the result is that sender and receiver end up with an identical random number which can be used as a key.

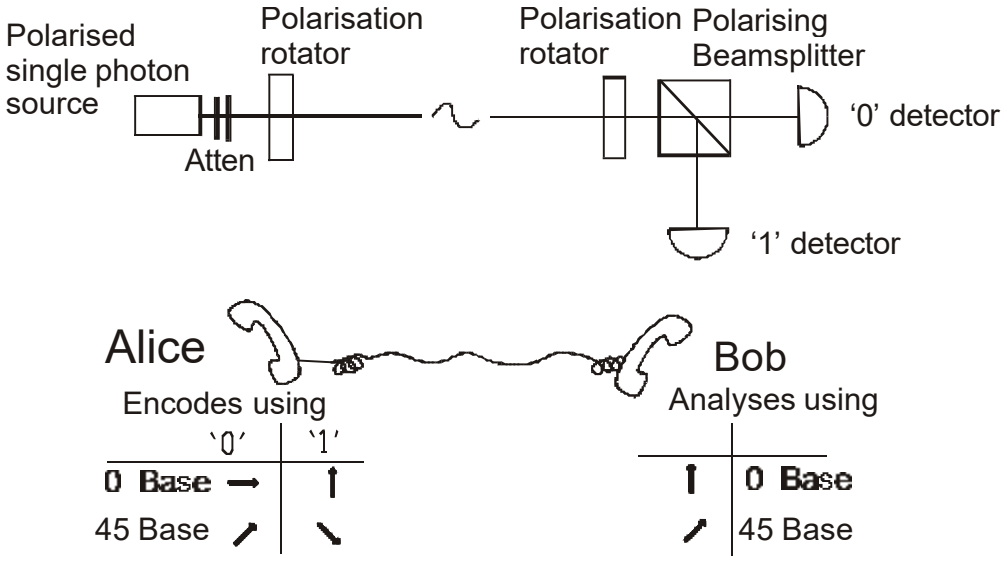


Fig. 1: The principle of quantum cryptography. Illustrated is the BB84 [1] protocol which utilises weak polarised pulses. Security is guaranteed when the coding base is randomly switched between 0 and 45 degrees using the polarisation rotators. When BOB measures in a different base no information can 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.

In a realistic system we do not have single photon sources. All experiments to date have been performed using weak light pulses to approximate single photon sources. When the mean number of photons per pulse drops to around 0.1 the Poisson distribution of photon numbers guarantees that the number of pulses with two photons is nearly negligible. We also expect the 'identical' raw keys will have errors and thus we need to implement secure error correction protocols [5,6] over the classical channel after key exchange.

3. THE BREADBOARD SYSTEM

The system is shown schematically in figure 2. We have selected a pulsed laser diode from Picoquant Gmbh which produces short (100ps) pulses of 635nm light at repetition rates up to 80MHz (we operate at 10MHz at present. Four acousto-optic switches are used to select randomly the four polarisations $0,45^0,90^0,135^0$ using fixed half wave plates. The four polarisations are then recombined and passed through a collimating telescope to the free space path. In the receiver the collected beam is reduced in diameter and split into two beams by a non-polarising 50/50 beamsplitter. The beams are then recombined in a polarisation beamsplitter before detection in one of two photon-counting detectors (EG&G: SPCM AQR121). One beam passes through a half-wave plate set to provide 45^0 of polarisation rotation and is delayed by 3ns with respect to the other. This allows discrimination of the two measurement bases by detection timing.

Send and receive optical boards are interfaced to two separate computers (Alice and Bob). In the Alice computer we have implemented a random number store which can be downloaded at 20Mbaud to an interface card which drives the acousto-optic switches at 10MHz. In the Bob computer a two channel timing card records the time of arrival of every photodetection. Both computers are referenced to oven stabilised 10MHz oscillators (stability 1 part in 10^8). A novel

sparse single photon timing scheme synchronises the clocks to sub-nanosecond precision (no bright pulses are used) and sets the start time for data transmission. After synchronisation a large number of random bits are sent and timing data for the received photo-pulses stored. From this timing data the measurement basis is ascertained from the 3ns delay. Key sifting and error correction protocols are implemented (in the LABVIEW programming language) operating over serial, ethernet or modem based data links between the computers.

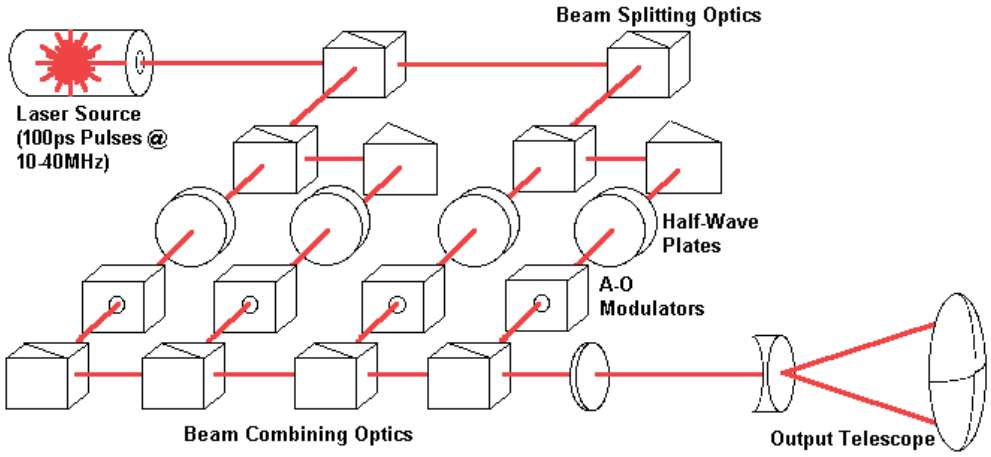


Fig. 2a Transmitter optics with four acousto-optically switched channels each with a fixed polariser.

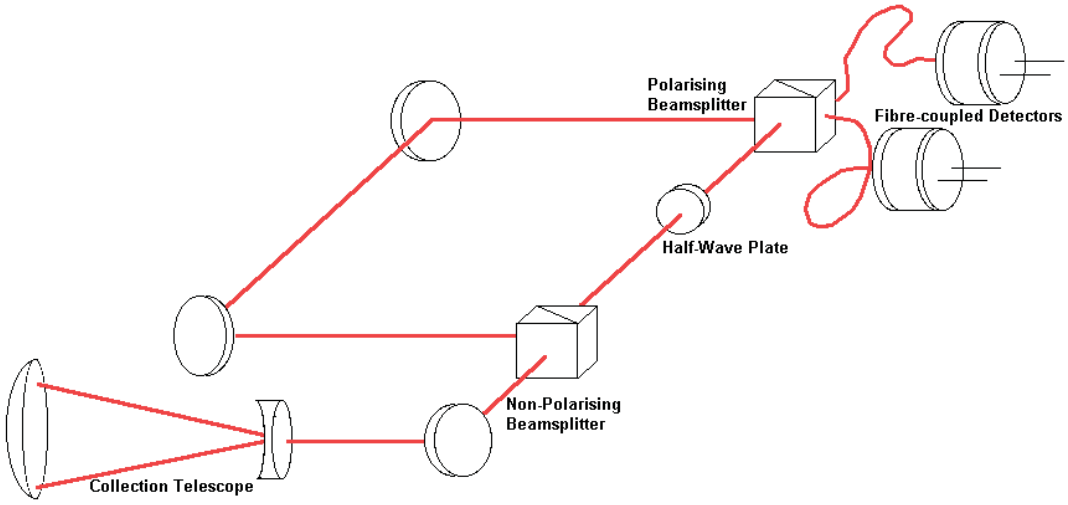


Fig. 2b Collection optics showing the randomising beam,splitter [2] that sets the measurement basis and the polarising beamsplitter measuring the bit value.

In a laboratory experiment we have been able to exchange keys at a rate close to 1 kilobit per second when simulating a 20dB transmission loss over the transmission path and operating at 0.1 photon per bit (this implies a receiver efficiency close to 10%). The fundamental limitation to the loss that can be tolerated is the background light and dark count in the detectors that leads to an unacceptably high error rate when bit rates fall below 1 kilobit per second. In an experiment at our 1.2km free space range we were able to demonstrate fully secure key exchange at 0.1 photon per bit at around 100 bits per second. The main reason for the poor long-range performance is the high degree of turbulence found on the ground based laser range. This led to beam wander up to

1mR and losses above 20dB. Work in progress on an elevated 1.9km beam path shows much lower turbulence (<100μR) and we expect to report secure key exchange imminently.

4. THE GROUND TO SATELLITE SCENARIO

The generic satellite system is shown schematically in figure 3. A satellite in low earth polar orbit will pass over a receiver station 1-3 times during the night before the earth rotates beneath. During these times a ground based tracking station will have a few minutes in which to lock on to the satellite and subsequently exchange keys. We have shown in our ground-based experiments that losses of 20dB can be tolerated. With careful design to reduce background counts and operating at night this could easily be raised to 30dB. We thus would like to aim for diffraction and atmospheric losses of order 25dB.

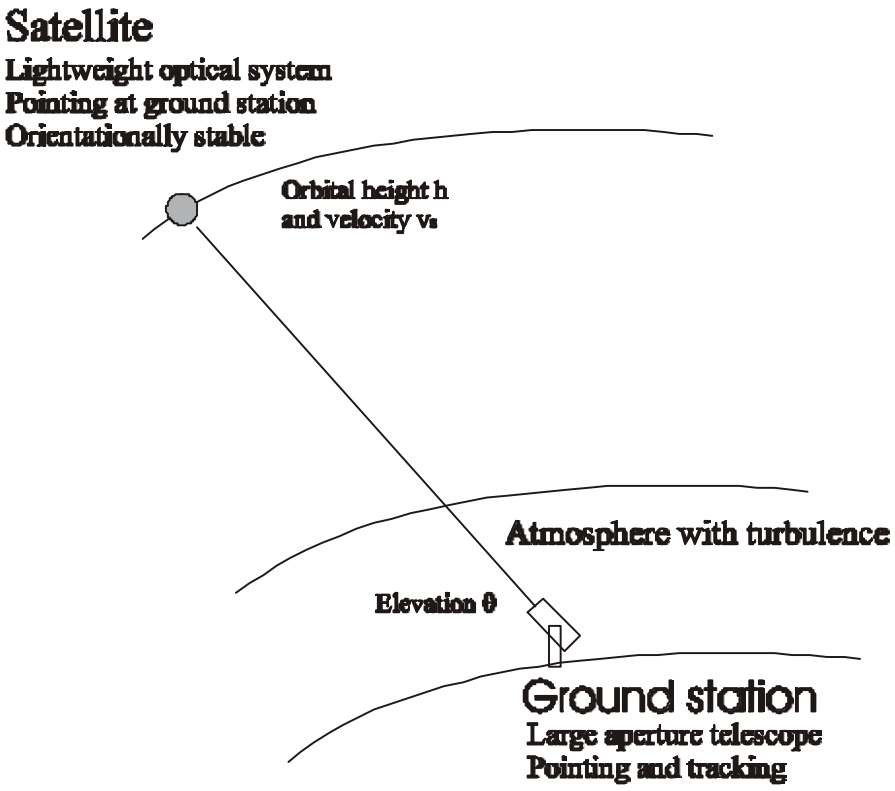


Fig. 3 Generic satellite QC experiment

We have considered three possible arrangements for key exchange to satellites based on the quantum cryptography technique.

A. Laser and encoding on the ground with detector on 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 polariser on the satellite.

At this stage we perceive a major problem with option A. due to diffraction losses and atmospheric turbulence induced beam wander which would restrict effective beam spread to a few tens of micro-radians. This implies a beam diameter of a few tens of metres at the satellite and losses of 30-40dB or heavy, large-diameter optics at the satellite. Option C. has the advantage of some compensation for beam wander due to retro-reflection but suffers from a doppler shift in the

return beam and requires a high speed polarisation modulator in the satellite. Wide field of view high speed modulators require heavy (10Kg) high voltage power supplies and may not be easily space qualified.

We find that the highest bit-rate and lowest launch mass could be obtained from option **B.** This option involves some risk associated with controlling, in space, laser wavelength and polarisation and in pointing from the satellite to the ground station with accuracy of order 10μR. Given the technical obstacles can be overcome we expect key exchange rates up to 10,000 bits per second when the satellite is at its closest approach to the ground station. With such a system we might expect megabits of key to be uploaded in a single pass. However we have restricted ourselves to operation in the dark as we suspect daytime operation will lead to error rates that are far too high.

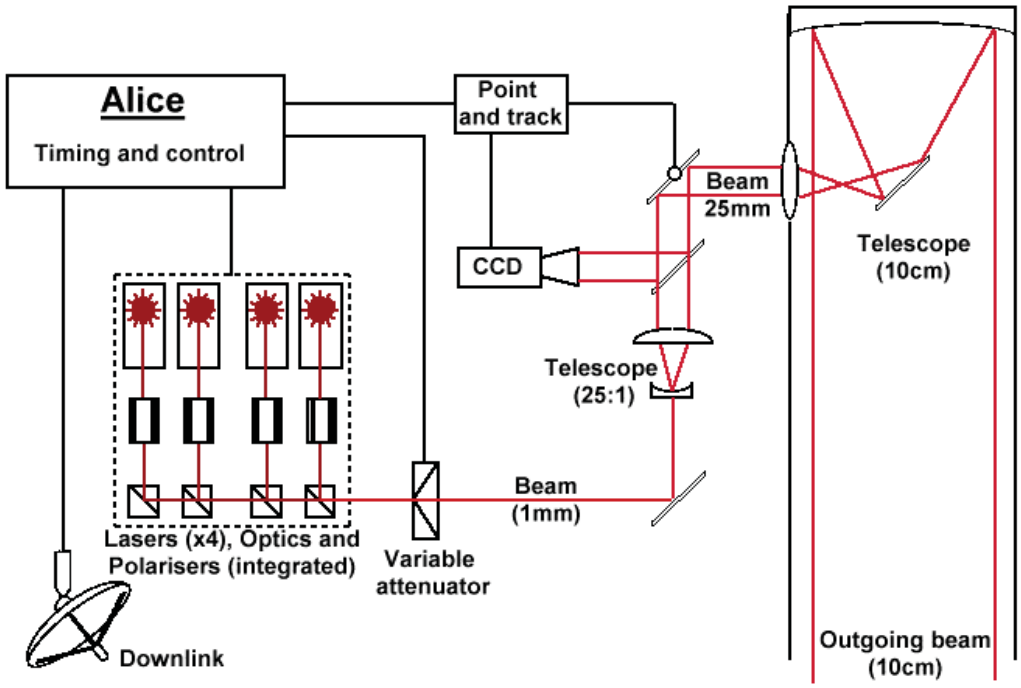


Fig. 4a: Satellite based transmitter. This includes a lightweight laser system using matched lasers and electronic switching between them to select the four polarisations used in the BB84 protocol. Pointing and tracking is controlled to the +/-0.5 degree level by the satellite while a closed loop system incorporating a CCD tracking electronics and tip-tilt mirror controls fine pointing to better than 10 μR.

In the proposed system the satellite optics (figure 4a) includes four wavelength-matched lasers pulsed at sub-nanosecond pulse-widths. Wavelength matching to 0.1nm would be achieved by selection of matched lasers from the manufacturer and careful temperature control on the satellite. Each laser would be used to encode one fixed polarisation and switching of polarisation could then be done by electronically switching between lasers allowing high modulation rates. The four beams would be recombined in polarisation insensitive beamsplitters. A computer switched attenuator would be needed to vary the pulse brightness. The high speed fine pointing control (+/-0.5 degrees) could be made by an intermediate tip-tilt mirror assuming some gross pointing accuracy of the satellite or external gimbal. The feedback loop would thus use a CCD camera to lock on to a bright laser on the ground station (to 10μR). We assume here a 10cm telescope with diffraction limit of order 8μR at an operating wavelength of 635nm. We are thus expecting 10-

20m footprint at ground level. This system could be made quite light-weight (<5Kg total mass) thus reducing launch costs.

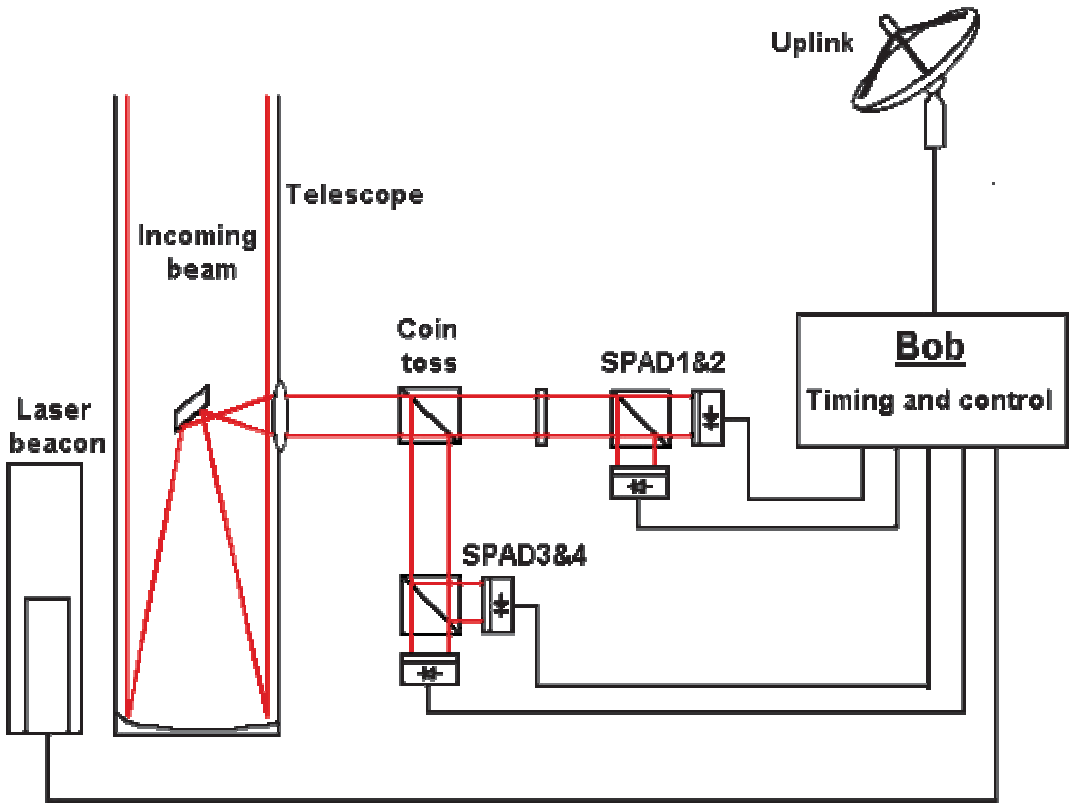


Fig. 4b: Ground station with telescope and boresighted beacon laser. The four detector receiver design incorporates a randomising beamsplitter [2] and provides the widest field of view (up to 100μR at the telescope output).

The receiver (figure 4b) is in the ground station which would allow the option of a 1m diameter telescope. To reduce tracking wander one can arrange the detectors to have of order 50μR field of view. Some form of active tracking using a beacon laser at the satellite may also be required. In this form daylight background levels will be high and night operation will be preferred. Tracking to better than 10μR should be possible on some high altitude ground stations. In this form the system then has a geometric loss budget around 20-26dB at 1000km range. Due to rotation of the satellite with respect to the ground station we would also have to implement some active polarisation control in the ground station to keep the bit error rate low. The key rate will be limited by the maximum repetition rate of the lasers. Initially we plan to use R=100MHz. Assuming we can reach the 20-30dB loss region we expect a ground key rate at 0.1 photon per bit of K~1000-10,000 bits per second. As we can expect a few minutes of viewing per pass the key length can extend to megabits. However the system as described has in principle no upper limit to the pulse repetition rate as long as the two systems can be time synchronised adequately. We expect synchronisation to better than 100ps to be possible in future allowing multi-gigahertz operation.

5. CONCLUSIONS

We have begun a study of free space quantum cryptography for secure key exchange. On a simple ground to ground system we have shown the key exchange can be demonstrated even with

transmission loss of order 20dB. To extend this principle to a satellite borne key exchange system we have to increase our loss tolerance to at least 30dB and incorporate the pointing and tracking technologies that have been developed for classical optical links between satellites.

REFERENCES:

1. C H Bennett et al, 'Experimental Quantum Cryptography', *J. Cryptology* **5** (1992) 3-28
2. J.G.Rarity, P.C.M.Owens and P R Tapster, 'Quantum Random Number Generation and Key Sharing', *J.Mod Opt* 41 (1994) 2435-2444.
3. W.T.Buttler et al, 'Practical Free-Space Quantum Key Distribution over 1km', *Phys.Rev.Letts*, **81** (1998) 3283.
4. W.T. Buttler, R.J. Hughes, S.K. Lamoureaux, G.L. Morgan, J.E.Nordholtand C.G. Peterson, 'Daylight Quantum Key Distribution Over 1.6km', *Phys.Rev.Letts*, **84** (2000) 5652-5655.
5. C..H. Bennett, G.Brassard and J-M Robert, Privacy Amplification by Public Discussion, *SIAM Journal on Computing*, **17**, (1988) 210-229
6. G.Brassard and L.Salvail, 'Secret Key Reconciliation by public discussion, Adventures in Cryptology', *EUROCRYPT93, Lecture Notes in Computer Science*, **765,** Springer-Verlag. N.Y. (1994) 410-423