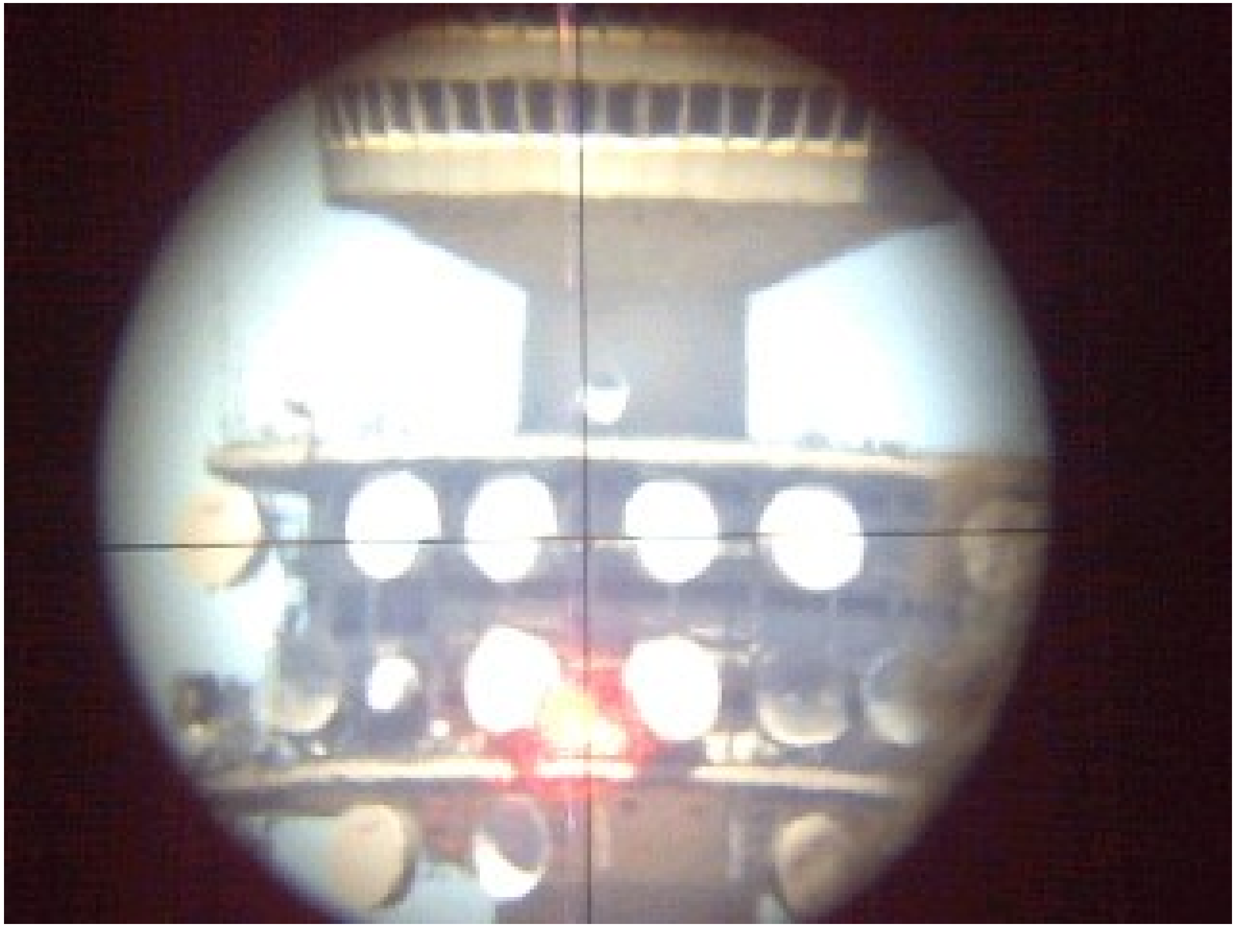
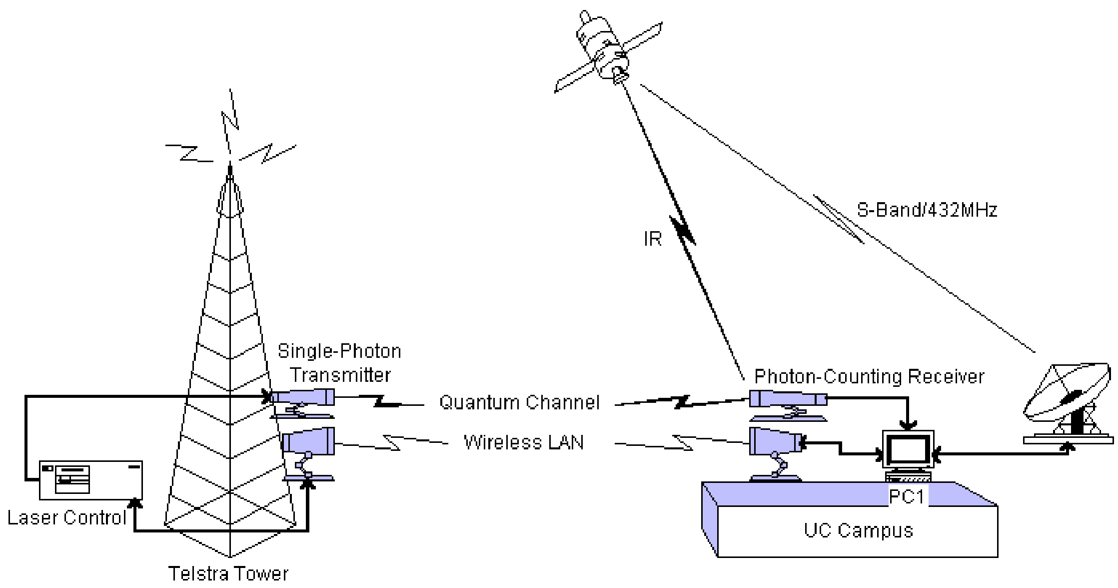
Forth in Research

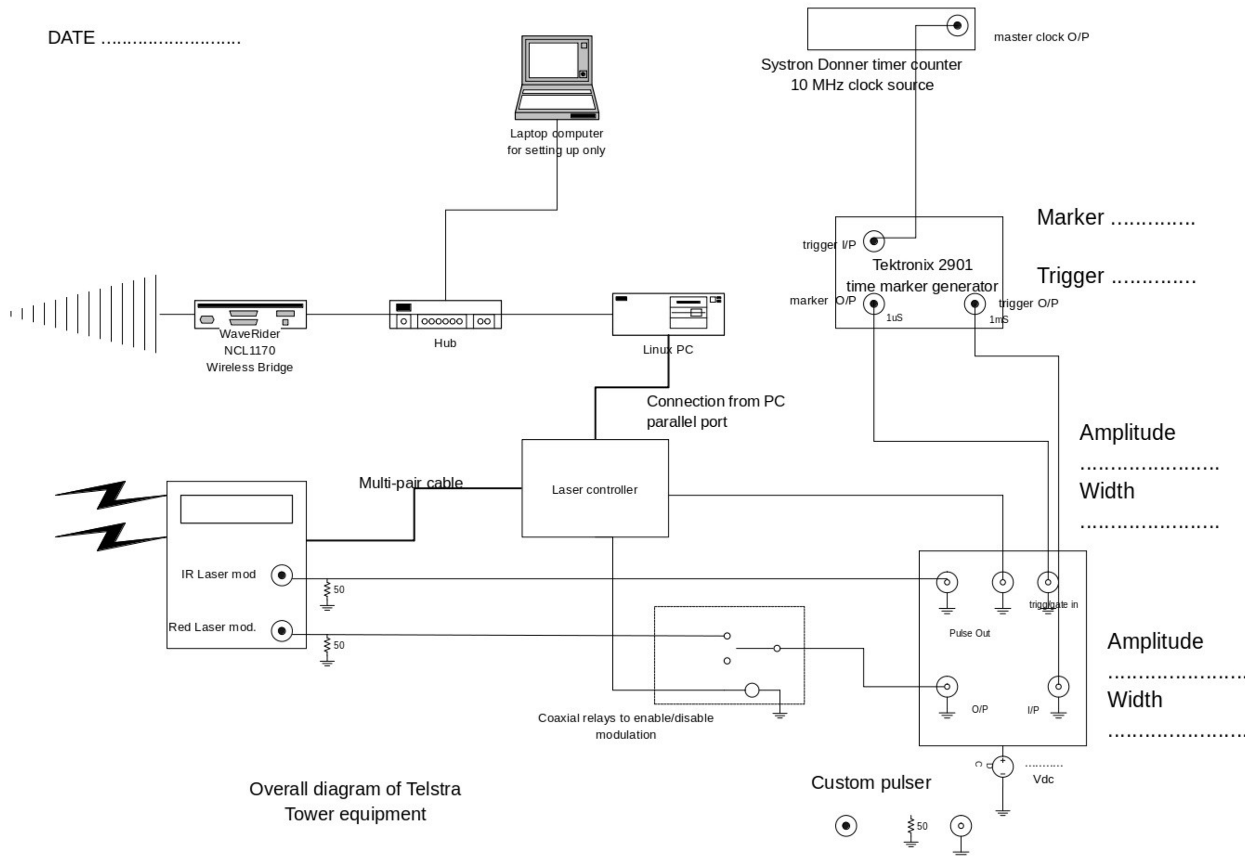
Quantum key cryptography for free space optical communications

Telstra Tower Canberra



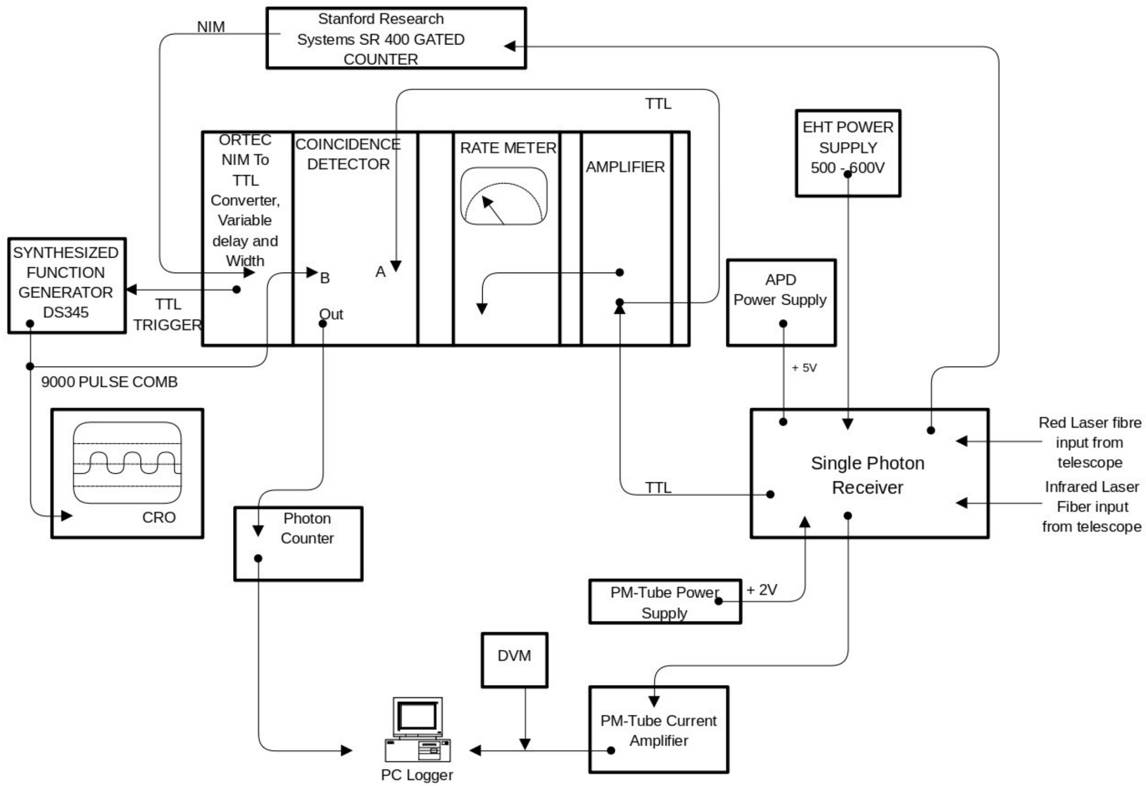


S-Band/432MHz
IR
Single-Photon
Transmitter
Quantum Channel
Wireless LAN
Photon-Counting Receiver
Laser Control
Telstra Tower
PC1
UC Campus



Overall diagram of Telstra
Tower equipment

The back end of the telescope



NIM
Stanford Research Systems SR 400 GATED COUNTER
TTL
EHT POWER SUPPLY 500 - 600V
ORTEC NIM To TTL Converter, Variable delay and Width
COINCIDENCE DETECTOR
RATE METER
AMPLIFIER
SYNTHESIZED FUNCTION GENERATOR DS345
B
A
Out
TTL TRIGGER
APD Power Supply
+ 5V
9000 PULSE COMB
CRO
Photon Counter
TTL
Single Photon Receiver
Red Laser fibre input from telescope
Infrared Laser Fiber input from telescope
PM-Tube Power Supply
+ 2V
DVM
PM-Tube Current Amplifier
PC Logger

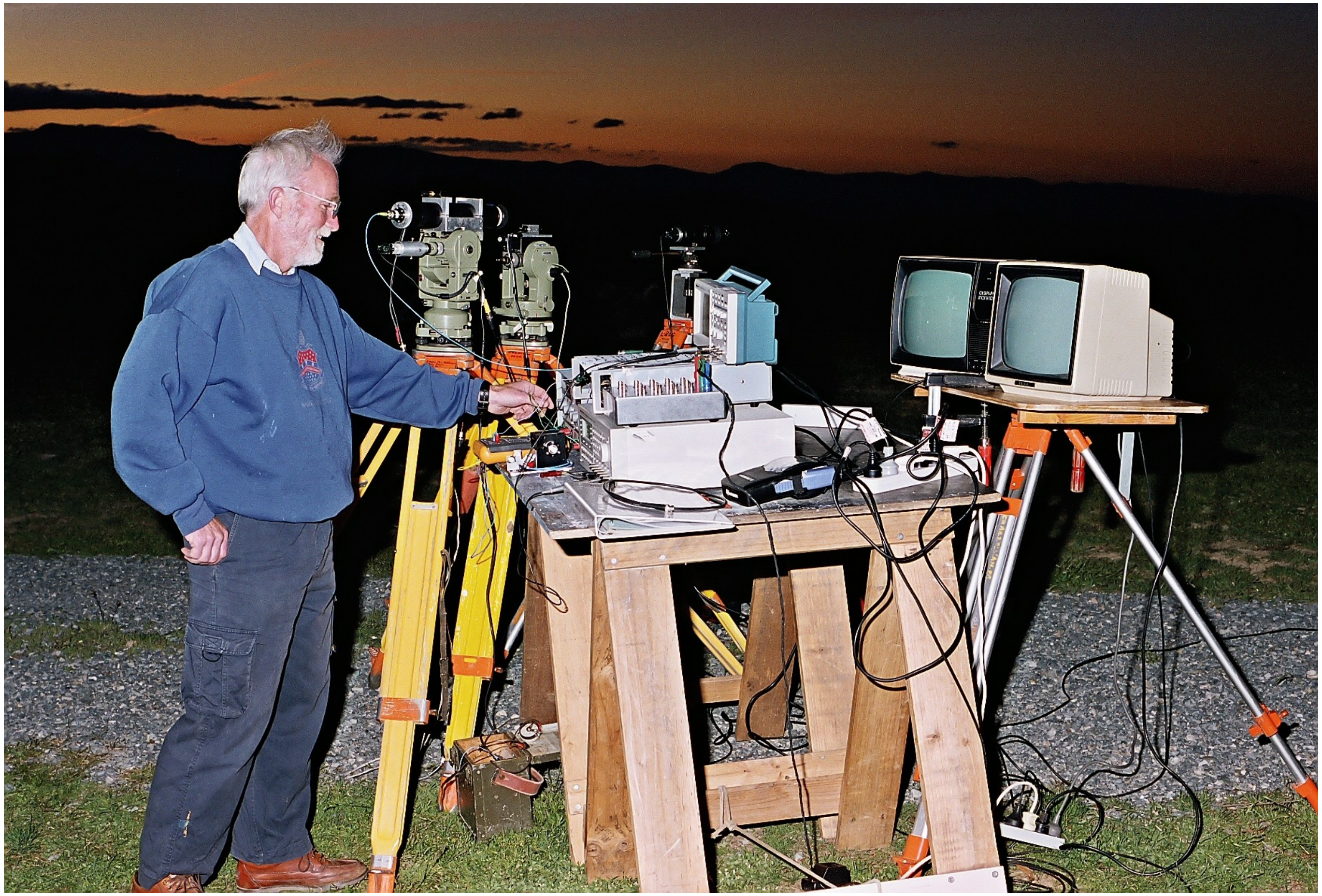
Start of Forth code

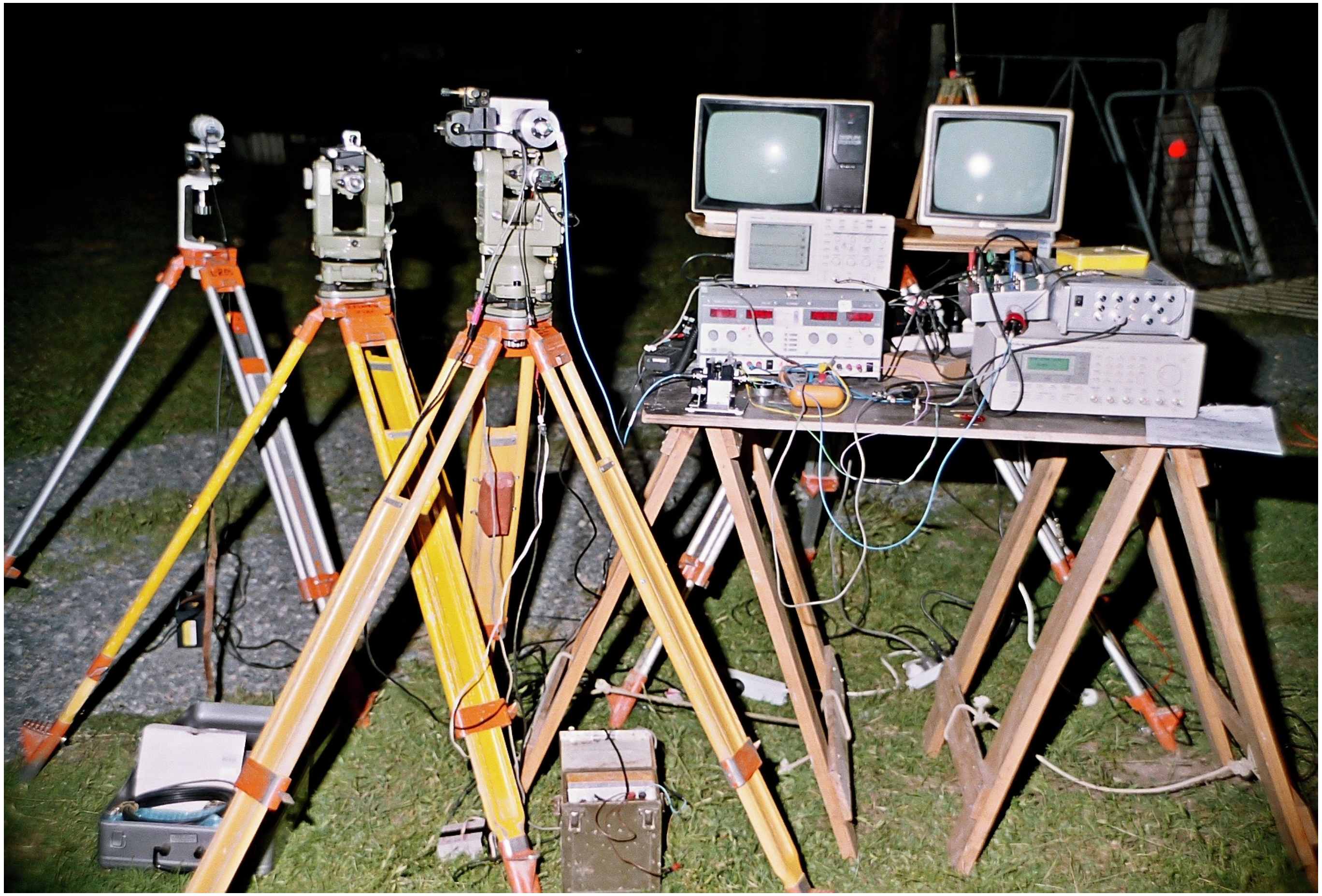
```
#! /usr/local/bin/gforth

\ pport.fth     Parallel Port i/o for the PC
\ Adapted from the work by Skip Carter 1996
\ see FD Vol XVIII Number 3

s" /home/ucan/control/ports.fth" INCLUDED
: initialise ( -- )     \ open up the parallel I/O port
        init-port TO #IOPORTS
;
HEX

378     CONSTANT #DATA

DECIMAL

128     CONSTANT POWER
1       CONSTANT RED_LASER
2       CONSTANT FLASHER
4       CONSTANT SPARE
8       CONSTANT GREEN_LASER
16      CONSTANT IR_LASER
32         CONSTANT LASER_POWER
300     CONSTANT DOTSPEED
VARIABLE #DATABYTE

\ ==============================================================

#DATA 1+        CONSTANT #STATUS
#DATA 2 +       CONSTANT #COMMAND
0 #DATABYTE !
```

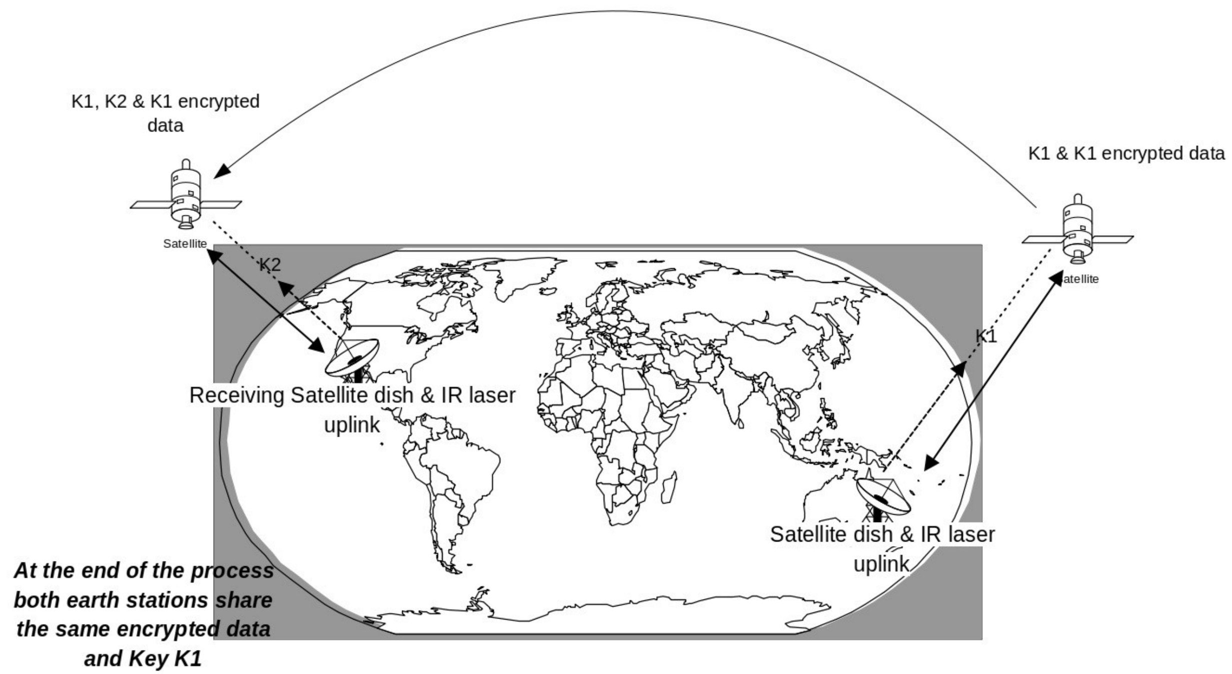
End of forth code

```
: SELECT
        BEGIN
        15 1 DO CR LOOP
\        #DATABYTE .bit-values CR CR

        ." Enter one of the following "    CR CR
        ." 0 to clear all bits, power OFF" CR CR
        ." 1 flasher on "   CR CR
        ." 2 flasher off "   CR CR
        ." 3 red laser on " CR CR
        ." 4 red laser off " CR CR
        ." 5 green laser on " CR CR
        ." 6 green laser off " CR CR
        ." 7 IR laser on " CR CR
        ." 8 IR laser off " CR CR
." H laser, HIGH power " CR CR
." L laser, LOW power " CR CR
        ." 9 Power on " CR CR
        ." ESC to teminate " CR CR

                KEY DUP
                CASE
                        48 OF kill_all ENDOF
                        49 OF FLASHER SETBIT ENDOF
                        50 OF FLASHER RESETBIT ENDOF
                        51 OF RED_LASER SETBIT ENDOF
                        52 OF RED_LASER RESETBIT ENDOF
                        53 OF GREEN_LASER SETBIT ENDOF
                        54 OF GREEN_LASER RESETBIT ENDOF
                        55 OF IR_LASER SETBIT ENDOF
                        56 OF IR_LASER RESETBIT ENDOF
                        57 OF POWER SETBIT ENDOF
                       104 OF LASER_POWER SETBIT ENDOF
                       72 OF LASER_POWER SETBIT ENDOF
                       108 OF LASER_POWER RESETBIT ENDOF
                       76 OF LASER_POWER RESETBIT ENDOF

                         ENDCASE
        ESC =
        UNTIL
        kill_all
;

kill_all SELECT
```

Receiving station

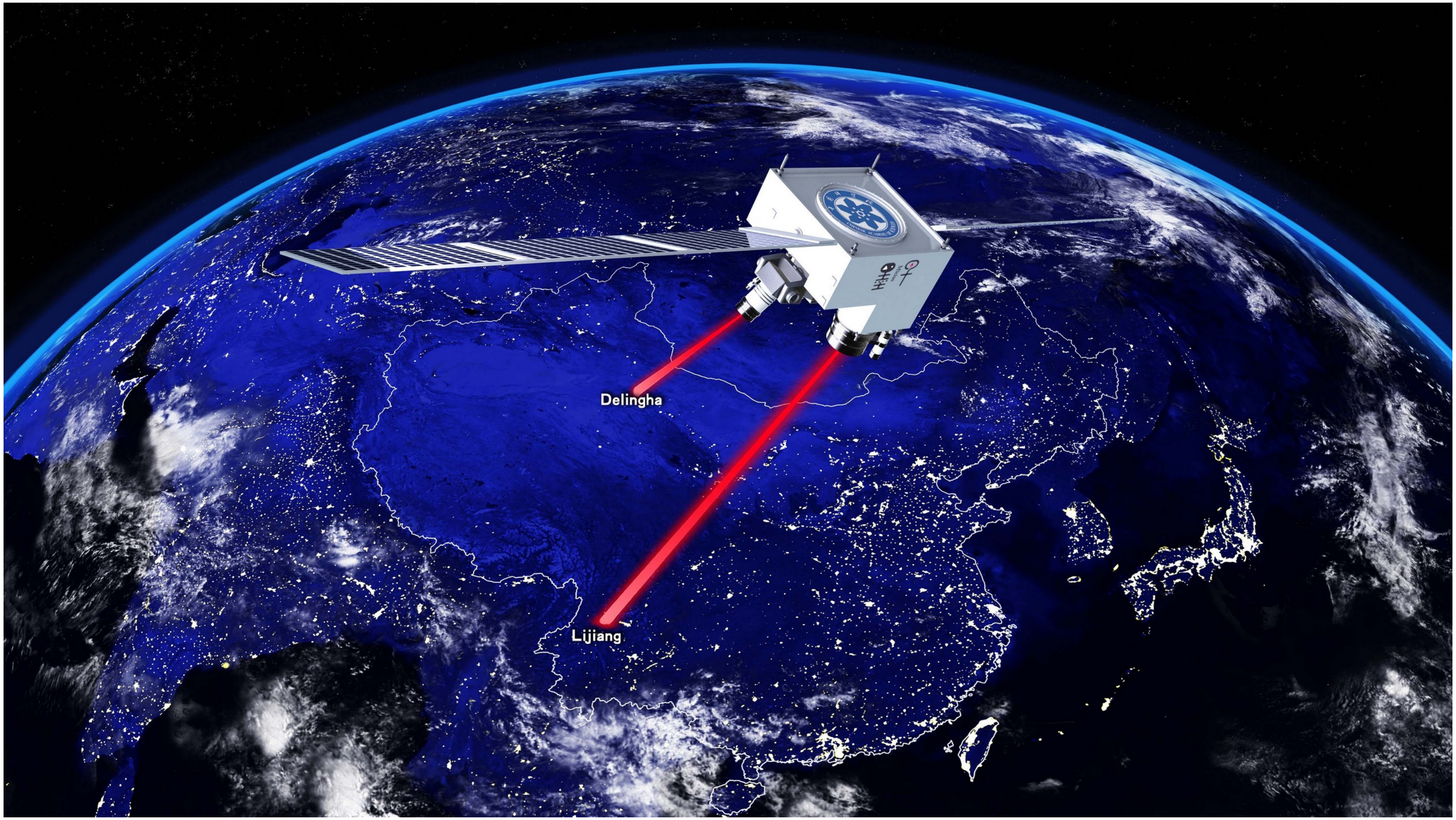






Quantum Key Transfer by Satellite

n channel on IR laser uplink - Cryptographic Keys (K1, K2)


Delingha
Lijiang

Several published papers

QUANTUM COMMUNICATION TRIALS OVER LONG ATMOSPHERIC PATHS

Paul Edwards, Adrian Blake, C. Cochran, Jeremy Gleeson, Ian Lisle, Adrian Thearle, Adrian Whichello, David Woodgate, Peter Zelman; Centre for Advanced Telecommunications and Quantum Electronics Research, Division of Business, Law and Information Sciences, University of Canberra, Canberra, ACT 2601, Australia; *paule@ise.canberra.edu.au;adrian.blake@ieee.org;cochran@webone.com.au;jeremy.gleeson@netspeed.com.au;Ian.Lisle@canberra.edu.au;adrian@thearle.com.au;adrianw@ise.canberra.edu.au;David.Woodgate@canberra.edu.au; peterz@pcug.org.au.*

Introduction

There is current interest in high bit rate transmission of very weak optical pulses between earth stations and low earth orbit satellites as a means of distributing secret quantum cryptographic keys over global distances [1,2,3]. Atmospheric turbulence causes fluctuations in the phase and irradiance of bright cw signals and in the photon number, arrival times and shape of weak picosecond scale pulses [4]. Although the characteristic time scale for optical intensity ("scintillation") noise is typically a few tens of milliseconds, these latter effects limit the capacity of long path transmissions to less than 100 Gbps.

Long Path Measurements

We have investigated the propagation of both bright and weak red (635 nm) and IR (832 nm) cw and pulsed laser beams through the atmosphere. Our trials [1,3] have included the transmission of weak coherent linearly polarized pulses ("quasi-qubits") in which the mean photon number occupancy <<1, a requirement for secure quantum key bit distribution, over distances between 4 and 40 km.

The normalized bright beam variance $\sigma_I^2 = (\langle I^2\rangle - \langle I\rangle^2) / \langle I\rangle^2$ is typically between 0.3 and 0.7, with little dependence on path length. The bright beam irradiance distribution is lognormal. We have successfully modeled the measured doubly stochastic photon count distribution from Poisson-transformed bright beam data [2,5] and also the bit error run distribution, relevant to quantum key bit error correction.

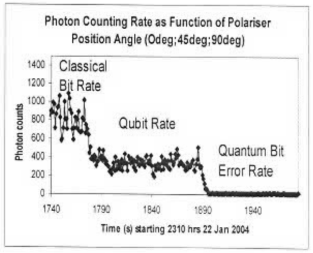


Fig. 1: Linearly polarised single-photon pulse counting rates: B92 protocol single-channel quantum key simulation over 26 km path.

References

1. P. J. Edwards, P. Lynam, C. Cochran, A. Blake, "Simulation of ground-satellite quantum key exchange using a dedicated atmospheric free-space testbed," in *Quantum Communications and Quantum Imaging*, edited by Ronald E. Meyers, Yanhua Shih, Proceedings of SPIE Vol. 5161 (SPIE, Bellingham, WA, 2004), pp.152-160, 2004.
2. P. W. Milonni, J. H. Carter, C. G. Peterson and R. J. Hughes, "Effects of propagation through atmospheric turbulence on photon statistics", to be published in *Quantum and Semi-classical Optics*, 2004.
3. P. J. Edwards, A. Blake, C. Cochran, J. Gleeson, H. B. O'Keeffe, D. Woodgate and P. Zelman, "Free-space quantum bit transfer over a 26 km urban path", www.ips.gov.au/IPSHosted/NCRS/wars/wars2004/, (Abstract only), Workshop on Applications of Radio Science, WARS 04, Australian National Committee for Radio Science, Hobart, Feb. 2004.
4. P. J. Edwards and A. Whichello, "Propagation noise in broadband free-space optical communication systems", Invited Paper 5473-13, presented at 2nd SPIE International Symposium on Fluctuations and Noise, Maspalomas, Gran Canaria, Spain, *SPIE Proceedings FN07*, May 2004.
5. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press, New York, 1995.

Simulation of ground-satellite quantum key exchange using a dedicated atmospheric free-space test-bed

Paul J Edwards, P. Lynam, C. Cochran and A. Blake

Centre for Advanced Telecommunications and Quantum Electronics Research, Division of Business, Law and Information Sciences, University of Canberra, Canberra, ACT 2601, Australia

ABSTRACT

The University of Canberra and its research collaborators have established a dedicated free-space laser communications test-bed between a national telecommunications facility and four selected monitoring sites at distances ranging from 4 to 47 km. This test-bed is currently being used to simulate and characterise the free-space quantum channel along which secure quantum key exchanges could take place between earth stations and low earth orbit satellites , the latter acting as global key couriers. We present the results of these trials conducted under a variety of atmospheric conditions. We use the results to estimate error rates and secure key exchange rates for ground/satellite key exchange systems employing weak Poissonian pulses with more stringent security requirements than are sometimes quoted.

Keywords: quantum cryptography, quantum key exchange, low earth orbit satellite, atmospheric turbulence, key security.

Quantum Satellite Micius extends Einstein's 'Spooky Action' to 1200 km

Initial results from the world's first quantum communications satellite Micius (Australasian Science, May/June 2017) launched last year have just been published (Science, 356, 6343, pp.1140-1144, June 16, 2017). They show unequivocally that the strange phenomenon of "quantum entanglement" between pairs of light photons survives to distances of at least 1200 km. This greatly extends the previous record of 100 km and is another nail in the coffin of Einstein's classical concept of physical reality. The results also strengthen the prospect of a secure global quantum internet, immune to hacking.

A secure quantum link established between two parties, traditionally called "Alice" and "Bob" in the cryptographic literature, allows them to share a cryptographic key without fear of eavesdropping by a third party ("Eve"). This private key can then be used as a "one-time pad" to securely encrypt subsequent communications over an ordinary public network.

The new results show that a measurement of the state of one entangled photon by either Alice or Bob can instantaneously determine the outcome of a measurement by the other party, even though they may be separated by thousands of kilometres. Alice and Bob can create a shared secret key by making a series of measurements on pairs of entangled photons. Interception of the key by an Eve will destroy the correlation between the two sets of measurements and be easily detected.

Micius carries a bright source on board that generates 6 million entangled photon pairs per second. It delivers them to Alice and Bob on the ground at a rate of one pair per second via a highly sophisticated laser acquisition, tracking and pointing system, a technical and scientific tour de force.

Results have been reported from two Chinese high altitude ground stations separated by 1200 km using large (greater than 1 metre diameter) optical telescope receivers: one at Delingha on the Tibetan plateau, the other at Lijiang in Yunnan province. The accompanying picture (Courtesy Prof. Jian-Wei Pan) shows the two satellite to ground down links to these stations in simultaneous operation.

The enormous (64-82 decibel) attenuation of the entangled photon-pair beams over distances of a thousand or more km from satellite to ground, together with atmospheric turbulence at low angles of elevation, impose major challenges. Because Micius is accessible to both stations for less than 5 minutes each night, potential quantum key data transfer is limited to a few hundred bits a day at most. Clearly Micius represents only the first step in the practical implementation of a global satellite-based quantum key courier system.

Paul J Edwards