

## THE UNIVERSITY OF CANBERRA – TELSTRA TOWER QUANTUM CRYPTO – KEY TELECOMMUNICATIONS LINK

Paul J Edwards

*Advanced Telecommunications and Quantum Electronics Research Centre  
University of Canberra  
[paule@ise.canberra.edu.au](mailto:paule@ise.canberra.edu.au)*

### ABSTRACT

The University of Canberra Cryptographic Key Link (UNCCKL), the first Australian free-space quantum crypto-key distribution facility, was officially opened in Canberra on Marconi Centenary Day, December 12 2001. The 4.2 km link between Black Mountain Telstra Tower and the University of Canberra campus is the longest single-photon quantum key test range in the world. It is being set up as a testbed to investigate and develop high bit rate technologies for the global distribution of quantum crypto-keys using low earth orbit satellites. UNC<sup>2</sup>KL is a joint venture between the UNSW at ADFA, the Canberra Institute of Technology and the University of Canberra. It is part of a multinational quantum cryptography project involving US, UK and Australian participants.

### INTRODUCTION

Quantum cryptography, quantum computing and quantum teleportation have become feasible [1,2] as a result of recent advances in quantum device engineering and quantum information theory. Of these three, quantum cryptography is closest to practical realisation [1]. One form of quantum cryptography uses secret keys exchanged in the form of streams of single polarisation-encoded photons transmitted over publicly accessible optical communication channels. Security is provided by the laws of quantum physics rather than by computational complexity as in the well known RSA crypto-system. These laws ensure that any attempt to intercept the key and measure the unknown quantum state (for example the polarisation) of individual photons inevitably introduces noise into the QKD channel and alerts the users to the presence of the eavesdropper and the potential loss of security [3].

### PRINCIPLES OF QUANTUM CRYPTOGRAPHY

Quantum cryptography uses a “one-time pad” – the so called Vernam cipher [4], which is exchanged between parties to a secure communication in the form of a “quantum key”. Quantum technology provides the means for generating, encoding, transmitting and detecting the single light quanta which constitute the key. Quantum physics, through the operation of the Heisenberg uncertainty principle and related laws, ensures that the quantum states of the encoded photons (and therefore the quantum key bits) cannot be freely copied. Quantum information theory places rigorous upper bounds on the leakage of Shannon entropy to potential eavesdroppers in the real-world situation of non-ideal transmitters, noisy channels and inefficient detectors.

Encryption using one-time pads is known to be absolutely secure providing the key itself is secure. However, the key pad must contain at least as many bits as the message to be encrypted and can only be used once. High key transfer rates are therefore required. A second restriction is that true “single-photon” transmitters are not yet practical [5]. Standard practice is to use very weak pulsed lasers instead. With these, there is a non-zero probability of a signal pulse containing more than one photon. This exposes the QKD system to certain types of sophisticated attack and sets an upper limit to the link attenuation and therefore to the distance over which a quantum key can be shared between parties with provably high security. Current technology limits this distance to several tens of kilometres of passive low-loss optical fibre.

In the B92 scheme devised by Bennett of IBM in 1992 [6] a non-orthogonal plane-polarised binary (“qubit”) alphabet is used to encode the key. The angle between the two linear polarization states is chosen to be 45 degrees. This introduces the vital element of uncertainty into the decryption process. It is essential that the angle not be 90 degrees (the orthogonal polarisation), because this would create completely insecure classical key bits. Eve (the eavesdropper) could then (in principle) make perfect measurements of the binary polarisation states of the transmitted photons by using a polarisation-sensitive beam splitter to select each polarisation state with certainty. She could then cover her tracks by retransmitting exact copies to Bob, the legitimate recipient of the secret key, who would be none the wiser to the resulting complete loss of security.

As each photon arrives, Bob, the recipient of Alice’s transmitted key, randomly sets his receiver to detect either a 1-bit or a 0-bit. He uses a pair of polarisers orthogonal to Alice’s so that a transmitted 1-bit has a 50 % probability of registering correctly in his “not 0-bit” detector and a transmitted 0-bit has a 50% probability of being correctly detected

## Extended Abstract

in his “not 1-bit” detector. At the conclusion of the key transmission, Bob communicates with Alice on an open channel and advises which of her randomly chosen sequence of key bits registered in either one of his two detectors. He does not of course publically reveal which detectors were activated. These bits then become their shared raw key which can be error-corrected in a subsequent dialogue at the cost of some loss of information. The maximum permissible bit error rate for this protocol is close to 4%.

### THE UNIVERSITY OF CANBERRA – TELSTRA TOWER QKD TEST-BED

There is currently strong international interest in developing the technology to transmit quantum keys over global distances at high rates to meet the increasing demand for high-security broadband international communications. There is also strong interest in developing secure “last-mile” extensions of existing broadband networks in the CBD and in military situations. Free-space ground to satellite, satellite inter-orbit and terrestrial point to point links using polarised photons have been widely discussed in these contexts [7].

Following our first Australian laboratory QKD demonstration in 1999, and subsequent single-photon transmissions over a 50 metre path at Mt Stromlo Satellite Tracking Observatory in 2000 [8,9], we have now set up an experimental free-space link between the University of Canberra campus and the Telstra Tower on Black Mountain [10].

The UnC<sup>2</sup>KL facility comprises pulsed infra-red, red and green semiconductor laser diode transmitters located on Telstra Tower 4 km from the university where a single-photon-counting receiving terminal is located. The two terminals are linked by a 10 Mbps half-duplex S-band wireless LAN bridge connected to the University of Canberra Ethernet. This facilitates the testbed function of the system by enabling remote control of the laser transmitters as well as providing real-time link characterization, bit-error diagnostics and privacy amplification of test key transmissions.

The single-photon receiving system currently consists of two separate 200 mm telescopes with 0.5 mrad fields of view, chosen as a compromise between ensuring reception in the presence of atmospheric turbulence on the one hand, and on the other, keeping the error-generating background photon counting rate to a tolerable level. The two telescopes are coupled by optical fibres to a central photon detection station where a photo-multiplier responds to bright frame sync pulses transmitted by a red (630 nm) diode laser and two silicon APDs register the polarized 835 nm single-photon pulses from an IR laser. Fig.1 shows a generic single-photon QKD transmitter and receiver in block form.

The system will be used to simulate the use of low earth orbit optical satellites as global quantum key couriers (as in Fig. 1) using state of the art single-photon generators [5], modulators [11] and receivers. The 4 km path is actually longer than is needed to show image motion due to turbulence-induced wave-front distortion similar to that expected in a ground to low earth orbit satellite link.

The rate at which the raw key can be transmitted, the quantum key transfer rate ( $R_{kt}$ ), together with the associated mean error probability per bit, the quantum key bit error rate (QKBER) are two important operating parameters [9]. The raw key transfer rate is given by,

$$R_{kt} \approx \varepsilon \eta_d R_k \langle n \rangle, \quad (1)$$

where  $\varepsilon$  is the coding efficiency (0.25 bits/photon for the non-orthogonal binary B92 protocol),  $\eta_d$  is the overall photon transmission factor (typically  $10^{-3}$  or less for a LEOS link),  $R_k$  is the transmitter pulse repetition (key) rate, and  $\langle n \rangle$  is the mean (Poisson distributed) photon number transmitted per pulse. For  $\langle n \rangle = 0.01$  photons per pulse, this gives a raw key transfer rate of only 25 kbps at  $R_k = 10$  Gbps. The importance of using ultra broadband modulators [11] is evident. We also plan to develop short range broadband free-space technologies for terrestrial use.

The test bed will also be used to trial the novel single-photon generators required to maintain security and efficiency in high loss QKD systems such as those using low earth orbit satellites. It can be shown [12] that the secure channel efficiency from Eqn.1,  $R_{kt}/R_k = \varepsilon \eta_d \langle n \rangle$ , cannot exceed  $\eta_d^2$  for conventional weak laser sources. This forces the use of exceedingly weak pulses or else greatly improved single-photon generators in which the probability of multiple photon pulses is strongly suppressed [12].

It has been argued [7] that the physical security associated with line of sight systems such as terrestrial point-to-point and LEOS satellite based systems allows the above restrictions to be relaxed. Others have argued that the security of quantum key channels should be guaranteed absolutely by the laws of quantum physics, rather than by propitious physical circumstances. Whichever of these views is adopted, free-space line of sight satellite-based quantum key distribution appears to be the only presently known way in which to build global QKD networks and we believe that the Telstra Tower test-bed has a useful role to play in this respect.

### ACKNOWLEDGEMENTS

We acknowledge with thanks the financial assistance of the Australian Research Council.

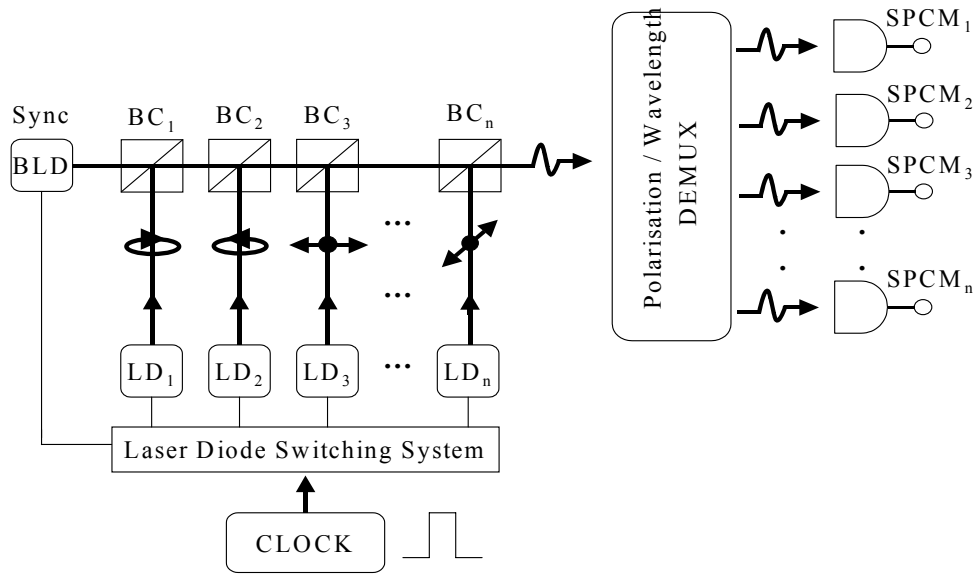


Figure 1. Block diagram of polarisation coded single photon WDM QKD transmitter and receiver. BC: Beam Combiner; SPCM: Single Photon APD Counting Module; LD: Laser Diode; BLD: Bright Laser Diode.

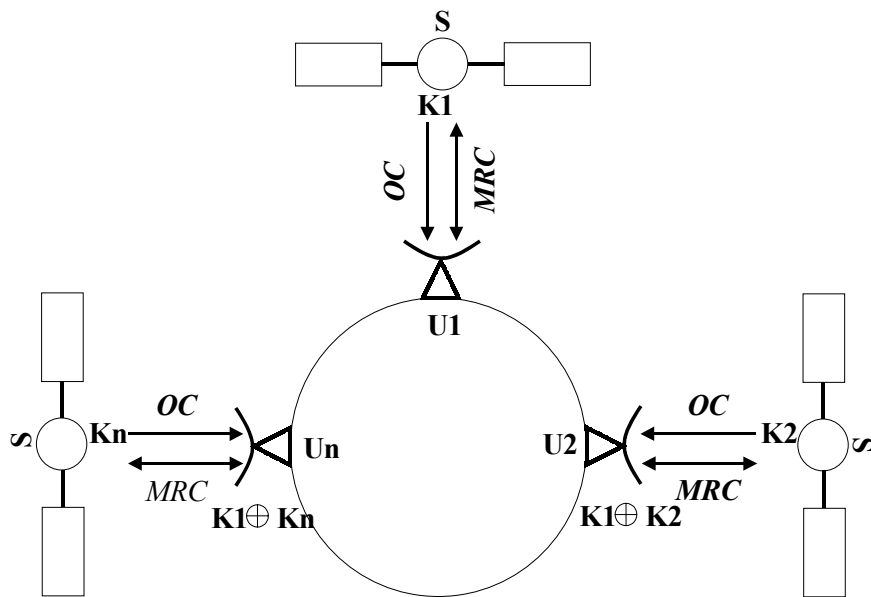


Fig. 2. Global quantum key distribution by satellite (S) using single-photon key distribution channels (OC); for key distribution and public microwave reconciliation channels (MRC) for the post key transmission dialogue.

## Extended Abstract

### REFERENCES

- [1] A. Zeilinger, W. Tittel, G. Ribordy, N. Gisin, D. Deutsch, A. Ekert, D. Vincenzo and B. Terhal, "Quantum Information", *Physics World*, pp. 33-57, March 1998.
- [2] P. J. Edwards, "Quantum communication and computation in the 21<sup>st</sup> century: the second century after Marconi", *IEEE Society Monitor* **20**, pp. 15-18, 1995.
- [3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography", *J. Cryptology*, **5**, pp. 3-28, 1992.
- [4] G. S. Vernam, *J. Amer. Inst. Electr. Engrs*, **45**, pp. 109-115, 1926.
- [5] J. Kim, O. Benson, H. Kan and Y. Yamamoto, "A single-photon turnstile device", *Nature* **397**, pp. 500-503, 1999.
- [6] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.* **68**, pp. 3121- 3124, 1992.
- [7] W.T. Buttler et alia, "Practical Free-Space Quantum Key Distribution over 1 km", *Phys. Rev. Lett.* **81**, 3283, 1998.
- [8] G. Ganeshkumar, P. J. Edwards, W. N. Cheung, L. O. Barbopoulos, H. Pham, and J. C. Hazel, "The University of Canberra quantum key distribution test bed", *12th Australian Optical Society Conf.*, p.34, University of Sydney, 1999.
- [9] P. J. Edwards, G. Ganeshkumar, W. N. Cheung and L.O. Barbopoulos, "Quantum cryptographic key distribution: A 21<sup>st</sup> Century technology", *ITEE Society Monitor* **25**, pp. 12-15, 2000.
- [10] P. J. Edwards and P. Lynam, "The University of Canberra –Telstra Tower Free-Space Quantum Key Distribution Testbed", *ITEE Society Monitor*, March 2002.
- [11] L. N. Binh and T. W. Chua, "Ultra Broadband Integrated Interferometric Optical Modulators", *Proceedings WARS 2002*, Leura NSW Australia (Feb 2002).
- [12] P. J. Edwards, G. H. Pollard and W. N. Cheung, "Quantum Key Distribution using Quantum-Correlated Photon Sources", *European Physical Journal D*, (in press, 2002).