Developments towards practical free-space quantum cryptography.

P R Tapster, P M Gorman, D M Benton, D M Taylor and B S Lowans
Qinetiq Ltd, (UK)

ABSTRACT

We describe a free space quantum cryptography system which is designed to allow continuous unattended key exchanges for periods of several days, and over ranges of a few kilometres. The system uses a four-laser faint-pulse transmission system running at a pulse rate of 10MHz to generate the required four alternative polarization states. The receiver module similarly automatically selects a measurement basis and performs polarization measurements with four avalanche photodiodes. The controlling software can implement the full key exchange including sifting, error correction, and privacy amplification required to generate a secure key.

INTRODUCTION

We have designed and built a quantum cryptography system which is intended to perform free space key exchanges at ranges of a few kilometres. The system has been designed specifically to be implemented quickly and easily. The Bob and Alice optical heads are compact and transportable. We use the BB84 protocol[1] and have implemented the full set of error correction and privacy amplification schemes in order to generate identical private keys at each end of the communication link.

RECEIVER HARDWARE

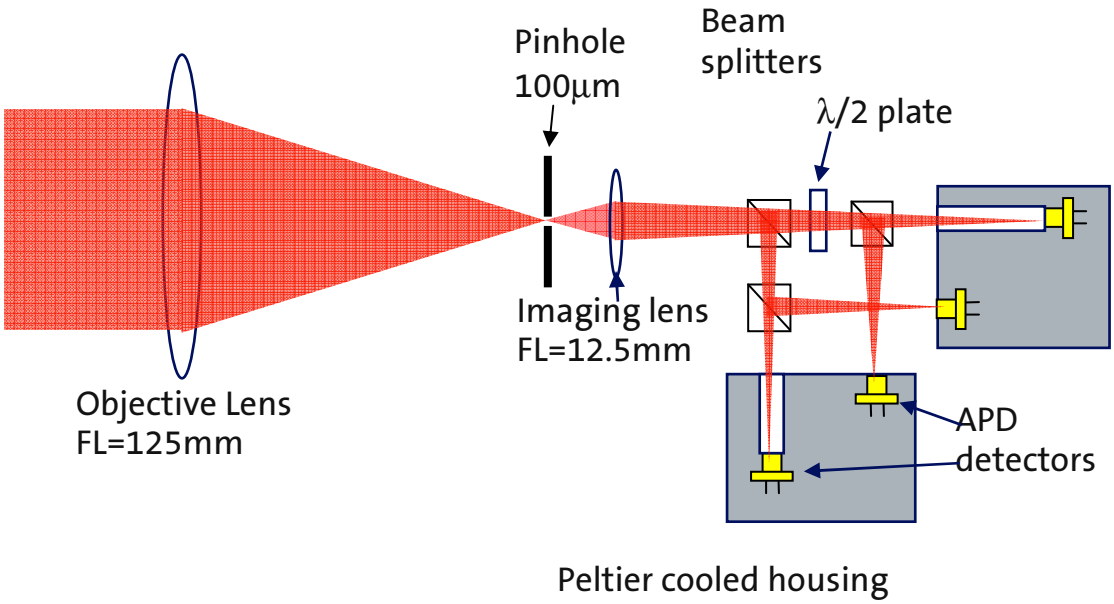

Figure 1. The optical arrangement of the receiver.

Our QKD receiver module was built by Ludwig Maximillian University, Munich. The optics is based on a standard beamsplitter design (Figure 1) Light from the transmitter module is collected by a 12.5 cm focal length objective lens and focussed by a 1.25 cm imaging lens. Between the lenses is a 100 micron diameter pinhole acting as a spatial filter. The primary purpose of this is to limit the sensitivity of the receiver module to ambient illumination.

Quantum Information and Computation III, edited by Eric J. Donkor, Andrew R. Pirich, Howard E. Brandt, Proceedings of SPIE Vol. 5815 (SPIE, Bellingham, WA, 2005)
0277-786X/05/$15 · doi: 10.1117/12.605539

After the imaging lens is the non-polarizing beam splitter. If an incoming photon is transmitted its polarization will be measured in the diagonal basis. This measurement is performed by the half-wave plate and polarizing beam splitter. At the output of the beam splitter are two photon counting silicon avalanche photodiodes (APD's) (Perkin Elmer C30902S) one of which finally detects the photon and determines the outcome of the measurement. If the incoming photon is reflected by the non-polarizing beam splitter then a second polarizing beam splitter and two more APD's perform a polarization measurement in the other basis.

Incorporated into the detection module are the electronics which performs various functions. The detectors are cooled by Peltier effect coolers and the electronics incorporate temperature controllers to stabilise detector temperatures. This helps to keep the dark count rate to the order of 700 /s. There is also a high voltage power supply, passive quenching circuitry and discriminators to generate a logic level pulse whenever a photon is detected. For compatibility with the hardware used to interface the detection events to the receiver computer, the four detector channels need to be reduced to two. This is done by delaying the pulses produced by one detector and combining them using an OR gate, with the pulses from another detector. Repeating this process generates two output channels each carrying pulses from two detectors. Since detections of photons emitted by the transmitter module should take place at specific times, it is possible to determine whether a pulse was delayed or not, and so reconstruct the outputs of four detectors from the two available channels. However, this cannot be done with events associated with dark counts or ambient illumination.

A GT658 card (Guide Technology Inc) is installed in a rack mount PC and the two timing inputs of the card are connected to the pulse outputs of the receiver module. The PC also contains a temperature controlled quartz crystal oscillator (TCXO) with a frequency stability of approximately one part in 10^9. This oscillator is used as the time base for the GT658 card, which can then measure the arrival time of each detection event with high accuracy.

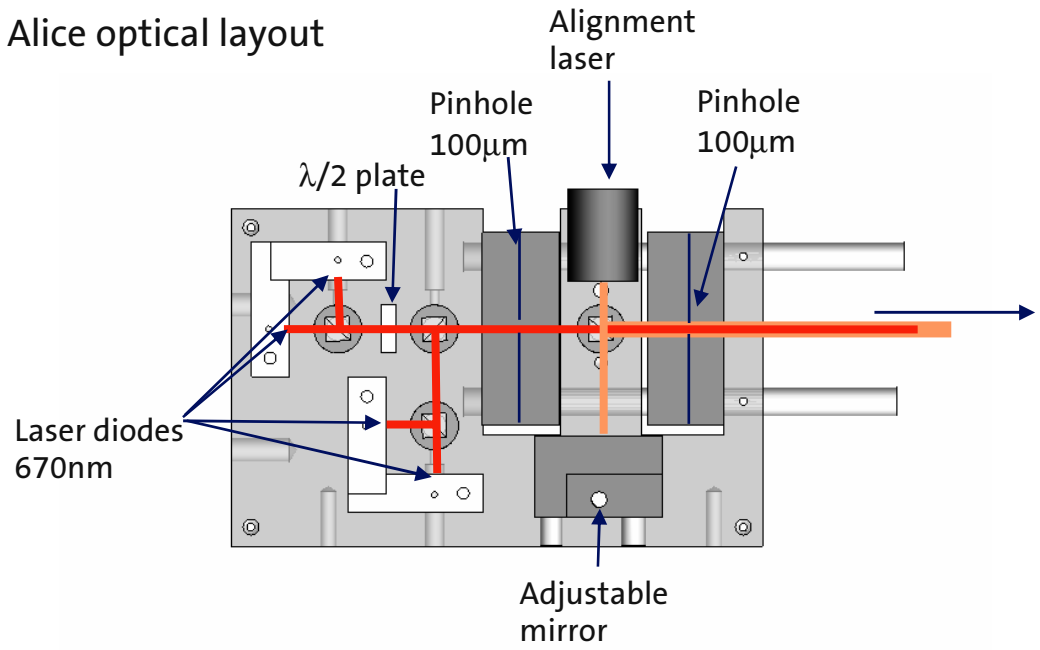

Figure 2. Optical layout of the Alice transmitter unit.

TRANSMITTER HARDWARE

Figure 2 shows the layout of the core transmitter optics. A pair of 670 nm laser diodes, one vertically polarized and one horizontally polarized, are mounted so that their output beams are combined by a beam splitter. A second similar pair are combined and the polarizations are rotated by a half-wave plate. A third beam splitter combines all four beams and passes them through a 100 micron diameter pinhole, followed by a second pinhole. The combination of two pinholes acts as a spatial filter which ensures that the output from each of the four lasers are in nearly the same spatial mode. The first pinhole also provides a substantial attenuation, bringing the intensity of each pulse down to a few photons per pulse.

An additional beamsplitter between the pinholes allows another laser to be introduced into the beam. This laser is focussed through the output pinhole and provides a higher intensity source used to align the transmitter and receiver modules; it is switched off during normal operation. Further to this the four laser channels can be operated in CW mode allowing alignment to be completed with a significant intensity of photons prior to pulsed operation, where alignment will be assured. A telescope with a magnification of 20 (not included in Figure 2) is used to reduce the divergence of the output. This should give a beam diameter of the order of 0.5m at a distance of 1km.

The transmitter head includes a printed circuit board which controls the laser output. Another TCXO similar to the one in the receiver PC provides an accurate 10MHz time base. An eight bit parallel connection from the PC is used to control high speed pulsing circuitry which delivers approximately 500ps pulses to the laser diodes. Normally one laser at a time is pulsed in a random sequence at 100ns time intervals, although all lasers can be pulsed simultaneously if required.

SOFTWARE

The PCs connected to the transmitter and receiver modules were provided with sufficient software to align and test the performance of the optics heads, as well as perform all necessary functions required for a quantum cryptographic key exchange.

The receiver system needs to be sufficiently synchronised to the transmitter so that it is possible to associate detection events with the individual pulse that caused it. This synchronisation process was performed in two stages. The receiver software maintains a virtual clock which runs continuously and is kept closely synchronised with the transmitter clock whenever a sufficiently large detection rate (above about 1000 events per second) is maintained. This is done by continually monitoring the arrival time of the detected photons and adjusting the rate of the software clock to maintain synchronisation.

The above procedure ensures that the software clock is running at the correct rate but is unable to distinguish one cycle of the clock from another. A common reference time is established by transmitting a header consisting of a fixed pattern of intensity modulation generated from a pseudo random bit sequence (PRBS). The detection rate is significantly lower than the transmission rate and the PRBS is repeated many times. The receiver correlates the detected time sequence with the expected PRBS intensity pattern and can determine the time at which the header finishes and the cryptographic data starts to be transmitted.

The software also performs the standard cryptographic functions required for a full key exchange. The sifting process identifies those photons which were successfully received and which were detected in the correct polarization basis. After restricting attention to these events, a raw key is available at each end of the system. The two keys will not be identical, because of errors caused by imperfections in the system and possibly the effect of eavesdropping attempts. It is then necessary to correct these errors by exchanging information while limiting the amount given away to those monitoring the public communication channel. This is done by using a variant of the Cascade algorithm[2]. At the end of the error correction process the original error rate is known exactly. Making the conservative assumption that the errors are caused by eavesdropping, an upper bound on the amount of information obtained by the eavesdropper can be obtained. As long as the eavesdroppers information is significantly less than the size of the raw key, it is possible to use privacy amplification techniques[3] to generate a shorter key which has no errors and which is effectively private. This means that the amount of information the eavesdropper has about the new key is negligible. We have implemented such a privacy amplification process in order to produce the final key.

RESULTS

The system has been tested at short ranges (4m) and at the intermediate range of 40m. At the intermediate range, using an intensity of 0.2 photons per pulse from the transmitter, the receiver detected raw key at a rate of over 12kbit/s and the quantum bit error rate (QBER) was 5.6% This corresponds to a final key exchange rate of more that 1kBit/s, after taking into account all the losses associated with the cryptography protocols, and also the limited duty cycle imposed by the software, which has to devote a certain amount of time to overhead activities. The result of QBER measurements from an extended trial over 40m is shown in figure 3.

In order to determine the reliability of the system, we allowed it to run unattended at short range for a period of two days. The data rates were observed to show changes of approximately 20%, but otherwise otherwise it was found that key exchanges could be performed reliably throughout the test.

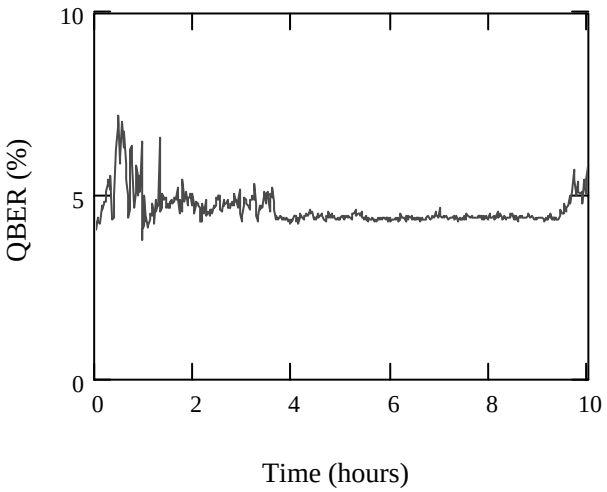

Figure 3. Results of key exchange tests over 40m.

REFERENCES

1 C H Bennett, G Brassard, "Quantum cryptography: public key distribution and coin tossing" *Int. Conf. Computers, Systems & Signal processing* pp175-179, Bangalore, India, December 1984

2 G Brassard, L Salvail, "Secret-key reconciliation by public discussion" *Workshop on the theory and applications of cryptographic techniques on advances in cryptology* pp 410-423, Springer-Verlag, 1994

3 C Bennett, G Brassard, J-M Robert, "Privacy amplification by public discussion" SIAM J Comp. **17**, 210-229