Quantum cryptography for multi-user passive optical networks

P. D. Townsend, S. J. D. Phoenix, K. J. Blow and S. M. Barnett*

BT Laboratories, Martlesham Heath, Ipswich, IP5 7RE, UK

* Department of Applied Physics, University of Strathclyde, Glasgow, UK

Abstract

Quantum cryptography has been shown to be an effective technique for the secure distribution of cryptographic keys on point-to-point communication links. Here, we describe adaptations of the existing quantum cryptography protocols and equipment configurations that allow secure key distribution to be performed on a variety of multi-user passive optical network (PON) architectures. These adaptations enable the network controller on the PON to distribute individual secret keys to each user on the network, and hence to securely encrypt subsequent data transmissions broadcast on the network.

Introduction: The concept of quantum cryptography, a theoretically secure technique for distributing cryptographic keys, was developed in the 1980s by Bennett, Brassard, Weisner and coworkers [1]. Their work culminated in a remarkable proof-of-principle demonstration of secure quantum key exchange over short distances of free space [2]. Since this original experiment progress towards practical applications has been rapid, with several studies showing the feasibility of using the technique over long distances in optical fibres [3-6]. We have recently taken this work a step further with the demonstration of a prototype system at BT laboratories that is capable of key transfer over distances of 10km in optical fibre at potential data rates of 20kbits/s [7]. With the expected improvements in single photon detector technology for the 1.3 and 1.5μm telecommunications windows quantum cryptography is set to become a potentially important technique for enhancing the security of data on optical communications systems.

In order to find widespread applications, however, it is likely that the technique must be employed on networks with many users where communications of the type *any-to-any* and *any-to-many* can occur. In contrast, the conventional application of quantum cryptography is to establish a secret key between a *single* transmitter and receiver pair joined by a fibre link as shown in figure 1a, and the quantum cryptography protocols developed to date [2, 3, 8-10] have been designed to protect this type of *one-to-one* communication. In this Letter we describe how multi-user operation can be achieved on fibre-distributed networks, with a variety of architectures, by means of simple adaptations of the original protocols and equipment configurations. The schemes allow a network controller to distribute distinct secret keys to each of N users on the network, and hence to securely encrypt subsequent data transmissions broadcast on the network.

Quantum Key Distribution on Branched Networks

One example of a multi-user network that is important in telecommunications is the star architecture shown in figure 1b, however, other configurations such as branch, tree, bus, or ring networks can also be employed. Many current applications of these network structures in, for example, computer LANs, local-access telecommunications networks,. and cable television distribution networks, use an electrical transmission medium such as coaxial cable or copper wire twisted pairs. However, the huge bandwidth available with optical fibre is leading to an increasing role for networks employing an optical transport layer. The latter is, of course, a basic requirement for quantum cryptography since the technique exploits the properties of photons.

In principle, communications in an optical network may be switched by means of, for example, spatial or wavelength routing devices, thus allowing optical paths to be dynamically established between any two terminals on the network. In this case, since an optical path exists between the terminals it is possible to use the standard point-to-point technique for quantum key distribution. However, there are important control issues to be solved with such complex networks, especially when the number of users N is large. We shall be concerned instead with much simpler architectures based on passive optical networks (PONs) in which the nodes are passive optical splitters. In the case of the star network, shown in figure 1b, communications then take place via the controller or exchange at the head-end of the PON and information is broadcast to, and 'broadgathered' from, the downstream terminals on the network. In order to perform quantum key distribution on such a network, we exploit the particle-like properties of low intensity quantum fields at optical couplers.

These properties are graphically illustrated by a simple experiment in which faint optical pulses from a pulsed semiconductor laser (1300nm wavelength, 100kHz repetition rate) are propagated through a 50/50 fibre coupler which is connected to a pair of single photon counting germanium avalanche photodiodes [Rarity et al.]. The detection equipment records both the singles count rate from each detector, and the coincidence count rate from the detector pair, as the average photon number per pulse μ is varied by means of an optical attenuator. The experimental results in figure 2 show the measured ratio of the coincidence to singles count rates, and this is plotted against μ which is normalised to take account of the low detector quantum efficiency (~5%) [Townsend, Thompson]. In this form, the data represents the probability that a faint optical pulse containing on average μ photons is split into two by the 50/50 coupler. As the average photon number per input pulse decreases below 1 it becomes less and less likely that this will occur, and instead the pulse is routed to one or the other of the outputs in a statistically random fashion. This is a manifestation of the basic laws of quantum mechanics which dictate that single quanta, such as photons, can neither be split nor cloned [Wooters & Zurek].

Clearly, in a multi-terminal network containing a sequence of such couplers a given input photon can, therefore, only ever reach a single receiver, not multiple receivers. The same is true, except with small probability, for optical pulses with $\mu \ll 1$, and these are much easier to generate in practice. Hence, in order to implement the standard quantum cryptography protocols on the network, the controller transmits a randomly encoded sequence of clocked pulses onto the network, and all receivers *simultaneously* make synchronous but independent random measurements on the network outputs. Because of the statistically random output from each coupler, this procedure is equivalent to simultaneously setting up N distinct quantum cryptography links in which the transmitter sends a different random sequence in each case. Of course the controller does not know in advance at which terminal a given pulse will be detected, however, this is taken care of in the public discussion phase of the protocol during which the controller sequentially polls each terminal on the network and performs a temporal correlation of the sent and received data as in the standard protocols . At the end of the process the controller has established a distinct secret key K_i with each terminal R_i on the network, and these keys can be used for two types of secure communication. In one-to-one communications the controller uses K_i to encrypt data signals intended only for R_i. Hence, although these signals are broadcast on the network and are therefore accessible to all receivers, only R_i can decode the data. In this scenario secure inter-terminal communications can still take place, however, the controller must act as a secure interpreter. Alternatively, the controller could use each K_i as the key in a one-time pad encryption of a master network key. This allows the master key to be securely distributed to each terminal on the network, and it can then be used to securely encrypt traffic between any of the users on the network with the controller performing only a routing function

.

Quantum Key Distribution on Looped Networks

The main functional units in the system are a single photon source and modulator in the transmitter, and a modulator and single photon detector in the receiver. In order to briefly explain the operation of this system we take the specific example of the original experiment performed by Bennett and coworkers [3]. In this scheme the transmitter sends the binary key data to the receiver via a clocked sequence of faint optical pulses, each of which is randomly encoded with one of four possible polarisations, namely -45_, +45_ (diagonal basis) and 0_, +90_ (rectilinear basis). These non-orthogonal basis pairs constitute two different representations of the binary digits 0, 1. During key exchange the receiver also switches randomly and independently between measurement polariser settings of -45_ and 0_. After the transmission, the transmitter and receiver communicate using a classical public channel in order to reconcile their data. This part of the protocol enables an error-free secret key to be established, even in the case of intermittent eavesdropping on the channel [1-3].

Conclusion: There are a wide range of applications for such network architectures, including e.g. optically-distributed computer LANs and local-access telecommunications networks, and in the future QKD may play an important role in providing high-levels of security in these areas.

Acknowledgements: Brassard

References

1 BENNETT, C. H., BRASSARD, G., BREIDBART, S., and WIESNER, S.: 'Quantum cryptography or unforgeable subway tokens', in *Advances in Cryptology : Proceedings of Crypto'82*, edited by CHAUM, D., RIVEST, R. L., and SHERMAN, A. T. (Plenum Press, New York 1983), pp. 267-275

2 BENNETT, C. H., BESSETTE, F., BRASSARD, G., SALVAIL, L., and SMOLIN, J.: 'Experimental quantum cryptography', *J. Cryptology*, 1992, **5,** pp. 3-28

3 BENNETT, C. H.: 'Quantum cryptography using any two nonorthogonal states', *Phys. Rev. Lett..,* 1992, **68,** pp. 3121-3124

4 HEISENBERG, W.

5 TOWNSEND P. D., RARITY J. G., and TAPSTER, P. R.: 'Single photon interference in a 10km long optical fibre interferometer', *Elect. Lett.,* 1993, **29,** pp. 634-635; 'Enhanced single photon fringe visibility in a 10km-long prototype quantum cryptography channel', *Elect. Lett.,* 1993, **29,** pp. 1291-1292

6 MULLER, A., BREGUET, J., and GISIN, N.:'Experimental demonstration of quantum cryptography using polarised photons in optical fibre over more than 1km', *Europhys. Lett.,* 1993, **23**, pp. 383-388

7 TOWNSEND, P. D., ''Secure key distribution system based on quantum cryptography', *Elect. Lett.*, 1994, **30**, 809-811

6 OWENS, P. C. M., RARITY, J. G., TAPSTER, P. R., KNIGHT, D. and TOWNSEND, P. D.: 'Photon counting using passively quenched germanium avalanche photodiodes', *Appl. Opt .(submitted),* 1993