Quantum Cryptography on Optical Fiber Networks

Paul D. Townsend

BT Laboratories,
B55-131D, Martlesham Heath, Ipswich, IP5 3RE, U.K.
paul.townsend@bt-sys.bt.co.uk

Abstract. The security of conventional or classical cryptography systems relies upon the supposed (but often unproven) difficulty of solving certain classes of mathematical problem. Quantum cryptography represents a new paradigm for secure communications systems since its security is based not on computational complexity, but instead on the laws of quantum physics, the same fundamental laws that govern the behaviour of the universe. For brevity, this paper concentrates solely on providing a simple overview of the practical security problems that quantum cryptography addresses and the basic concepts that underlie the technique. The accompanying talk will also cover this introductory material, but the main emphasis will be on practical applications of quantum cryptography in optical fiber systems. In particular, I will describe a number of experimental systems that have been developed and tested recently at BT Laboratories. The experimental results will be used to provides some insights about the likely performance parameters and application opportunities for this new technology.

1 Introduction

The information revolution of the latter half of the twentieth century has been driven by rapid technological developments in the fields of digital communications and digital data processing. A defining feature of today's digital information systems is that they operate within the domain of classical physics. Each bit of information can be fully described by a classical variable such as, for example, the voltage level at the input to a transistor or microprocessor. However, information can also be processed and transported quantum-mechanically, leading to a range of radically new functionalities [1]. These new features occur because the properties of quantum and classical information are fundamentally different. For example, while classical bits must take on one of the two mutually exclusive values of zero or one, quantum superposition enables a bit of quantum information to have the strange property of being both zero and one simultaneously. Furthermore, it is always possible, in principle, to read classical information and make a perfect copy of it without changing it. In contrast, quantum systems can be used to carry information coded in such a way that it is impossible to read it without changing it and impossible to make a perfect copy of it [2]. It is these

properties that are directly exploited in quantum cryptography [3–5] to provide secure communications on optical fiber systems [6–10]. The technique enables the secrecy of information transmitted over public networks to be tested in a fundamental way, since an eavesdropper will inevitably introduce readily detectable errors in the transmission. Quantum cryptography offers the intriguing prospect of certifiable levels of security that are guaranteed by fundamental physical laws. This possibility arises from the quantum nature of the communication system and cannot be realised with any conventional classical system.

2 Classical Cryptograhpy

In order to understand the problems that quantum cryptography addresses it is necessary to first review some background ideas from conventional or classical cryptography. Encryption is the process of taking a message or plaintext and scrambling it so that it is unreadable by anyone except the authorised recipient. This process is perhaps best described by a simple analogy. Encryption is the mathematical analogue of taking a message and placing it inside a lockable box. The box is then locked with a key held only by the sender and the authorised recipients of the message. Any unauthorised person intercepting the locked box will be unable to retrieve the message from the box without possessing a copy of the key.

Mathematically encryption can be described as an invertible mapping of a message $\mathbf{m}$ into a ciphertext $\mathbf{c}$. The mapping is achieved by an encryption algorithm, E, which takes as input the secret key, $\mathbf{k}$, and the message so that $\mathbf{c} = E(\mathbf{m}, \mathbf{k})$. The message, key and ciphertext are expressible as binary data strings. The decryption is achieved with the use of the inverse algorithm, D, so that $\mathbf{m} = \mathrm{D}(\mathbf{c}, \mathbf{k})$.

In terms of the lockable box analogy the algorithm is the locking mechanism which is activated by the key. As with the case of a mechanical lock it is the secrecy of the key that keeps the system secure. A well-designed lock should be difficult to open without the key even when the details of the lock are known. It is an accepted design principle of cryptographic algorithms that the security should not be dependent on the secrecy of the algorithm but should reside *entirely* in the secrecy of the key. A graphic example of this idea is provided by the 'one-time pad' cipher system [11] that was proposed by Vernam in 1926. In the binary version of the one-time pad encryption is performed by modulo 2 addition (equivalent to a bit by bit Boolean XOR) of the message and a random key of equal length. Despite the simplicity (and public availability!) of the XOR algorithm the one-time pad offers theoretically perfect secrecy as long as the key is kept secret and used only once [12]. In practice, the one-time pad is not widely used because of the requirement for large volumes of key data. However, most commercial algorithms, such as the Data Encryption Standard (DES), also use publicly available algorithms [13].

The requirement that the secrecy be entirely dependent upon the key also imposes another good design principle. In a practical system such as DES, that

does not offer the perfect secrecy of the one-time pad, an eavesdropper can always attack the system simply by trying each possible key in turn. A good algorithm will be designed such that this least efficient strategy is, nevertheless, the fastest method of attack. DES, for example, uses a key length of 56 bits so that an attacker performing an exhaustive key search will have to test, on average 2^{55} keys. Although this is a huge number, future increases in computational power will necessitate the use of longer keys.

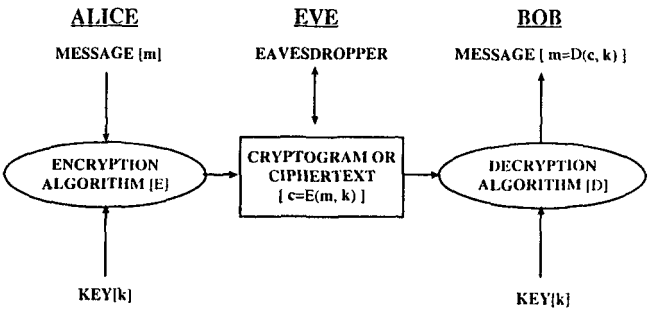

Fig. 1. The basic elements of a cipher system.

Figure 1 shows a schematic representation of a cryptography system, where the standard terminology of Alice, Bob and Eve is used to describe the transmitter, receiver and an unauthorised eavesdropper respectively. In order to operate the scheme Alice and Bob must exchange keys and, most importantly, must ensure that these keys do not fall into Eve's hands. Furthermore, if the system is to remain secure Alice and Bob must regularly repeat this process ensuring that the updated keys are also secret. How to achieve this goal is one of the central problems in secure communications; keys must be generated and distributed and the whole process managed in such a way as to ensure the secrecy of the system.

In essence quantum cryptography is a communication protocol that enables cryptographic keys to be securely distributed over communication channels that are physically insecure and hence potentially subject to eavesdropping. The technique achieves the desirable goal of an automated key establishment procedure between two or more parties in such a way that any unauthorised interception can be discovered and dealt with. Some modern cryptography systems attempt to solve the key management problems using a technique known as public-key cryptography [13]. In public-key cryptography each user has two keys, a private key, and a public key. The public key is widely distributed; the private key is kept secret. To send a confidential message using a public-key scheme Alice obtains Bob's public key from a public directory and uses this to encrypt her message to Bob. Once this has been done only Bob can decrypt the message using his private key. In terms of the lockable box analogy this is like having a box whose

lock is operated by two keys. Everyone has access to the key to lock the box but cannot unlock it. Only one key will open the box and that is the private key held by the message recipient.

The security of public-key cryptography systems is based on 'one-way functions' that is readily computable mathematical problems for which the solution of the inverse problem is thought to be computationally infeasible. The classic example of such a function is multiplication and its inverse factorisation. For example, it easy to multiply two large prime numbers, but extremely difficult to factorise the resulting product into its two prime factors. Cryptographers using public-key cryptography have to make the assumption that advances in mathematics and computing will not dramatically change the ability of an attacker to compute these difficult problems. This issue has received a great deal of attention recently because of Shor's discovery of a high-speed factorisation algorithm for quantum computers [14]. If such computers can ever be built, the security of public-key cryptosystems may be dramatically reduced.

3 Quantum Cryptography

3.1 Background

The following section describes the original 'BB84' quantum key distribution protocol developed by Bennett and Brassard [3]. This protocol is used exclusively in the BT experiments that will be described in the talk. In general, quantum information systems require the use of some suitable two-state quantum objects to provide quantum-level representations of binary information (qubits). In the BB84 scheme Alice and Bob employ the linear and circular polarization states of single photons of light for this purpose.Figure 2 shows schematic representations

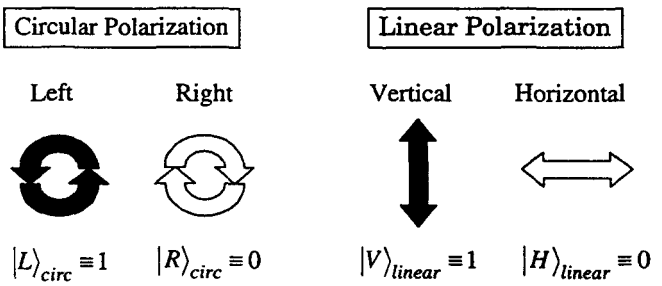

Fig. 2. Schematic representation and notation used to describe the linear and circular polarization states of single photons of light. In the BB84 quantum cryptography scheme the linear and circular states are used to provide two different quantum level representations of zero and one.

of these states together with the notation used to represent them and their associated binary values. The linear and circular 'bases' are used to provide two different quantum level representations of zero and one. Before describing how the properties of these single photon polarization states are exploited in the key distribution protocol we will consider the outcomes and interpretation of various possible measurements that can be performed on them.

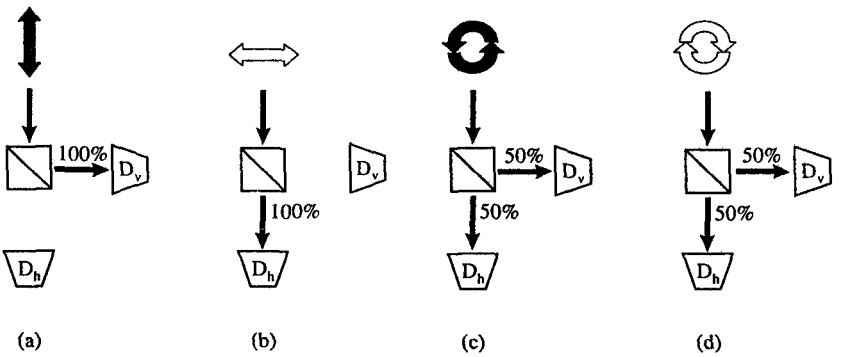

Fig. 3. A receiver uses a polarizer and two single photon detectors to perform linear polarization measurements on the linear (a and b) and circular (c and d) single photon polarization states. The probabilities of the various outcomes are indicated as percentage values. The linear measurement is incompatible with the circular representation and the photon is equally likely to be repolarized as either a horizontal or vertical state and detected at the appropriate detector.

Figures 3(a)-3(d) illustrate the possible outcomes of measurements on each of the four polarization states shown in figure 2. In each case the receiver has arranged a polarizer and two single photon detectors to perform a linear polarization measurement on the incoming photon (the apparatus is assumed to be perfect). For the two linear states the outcome of the measurement is deterministic, i.e. the $|V\rangle_{linear}$ photon is registered at detector D_V and the $|H\rangle_{linear}$ photon is registered at detector D_h, both with 100% accuracy. Of course similar results would also be obtained for classical input fields in the vertical and horizontal polarization states. In contrast, a classical input state with circular polarization would generate equal-intensity signals at the two detectors. Single photons, however, are elementary excitations of the electro-magnetic field and they cannot split in two. Instead the $|R\rangle_{circ}$ and $|L\rangle_{circ}$ states behave in a random fashion and have a 50% probability of being repolarized in the state $|V\rangle_{linear}$ and registered at D_V and, similarly, a 50% probability of being repolarized in the state $|H\rangle_{linear}$ and registered at D_h. In quantum mechanics terminology the photon is said to be projected into an eigen-state of the measurement operator, namely either $|V\rangle_{linear}$ or $|H\rangle_{linear}$. Taking the example of the $|R\rangle_{circ}$ state, the

probability of each possible outcome is given by the squared modulus of the amplitude coefficients in (1),

$$|R\rangle_{circ} = \frac{1}{\sqrt{2}(|V\rangle_{linear} + i|H\rangle_{linear})} \tag{1}$$

the expansion of $|R\rangle_{circ}$ in the linear representation. In the case of the current example it can be seen that the measurement provides no information at all on a photon's state of circular polarization. Of course, the receiver could have included a 1/4-wave retardation plate in front of the polarizer in order to perform a perfect circular measurement. However, this would only be obtained at the expense of no information on the photon's linear polarization state since the $|V\rangle_{linear}$ and $|H\rangle_{linear}$ states behave in a random fashion when subjected to a circular polarization measurement. This situation arises because linear and circular polarization are complementary quantum observables that are incompatible in the sense that a measurement of one property will always disturb the other. Consider now the situation where one of the four possible polarization states is chosen at random and the receiver is asked to distinguish which one has been sent. Evidently the receiver must choose a measurement to perform on the photon. If he happens to choose an incompatible measurement the outcome will be random, but this fact cannot be deduced from the measurement itself. Hence, the receiver cannot determine unambiguously the polarization state of the photon unless he is supplied with additional information on which type of state has been sent. All that can be said after a particular measurement is that the photon is now in the polarization state measured. Although we have used the example of a specific type of measurement here, there is in fact no single measurement or sequence of measurements that will allow the receiver to accurately determine the state of the photon when he is told only that it has been coded in one of two incompatible representations, but not which one. As we shall see, this peculiarly quantum phenomenon can be directly exploited to provide security in a quantum cryptography scheme. The reader might be tempted to suggest at this point that a solution to the measurement problem could be to copy the photon so that the receiver could measure different properties on the identical copies. Fortunately, at least from the quantum cryptographer's point of view, this type of 'cloning' is forbidden by quantum mechanics [2].

3.2 Quantum Key Distribution Protocol

The aim of quantum key distribution is not to take a specific predetermined key and send it to the recipient but rather to generate a random bit sequence in two separate locations that can then be used as a key. The key only comes into existence when the entire protocol has been executed. In order to carry out this process the transmitter Alice and the receiver Bob employ a pair of communication channels: a quantum channel that is used for sending the photons and a classical channel that is used for a subsequent public discussion about various aspects of the quantum transmission. It is assumed that Eve may have access to

both of these channels at any time. She may make any measurement that she chooses on the quantum channel and is free to learn the contents of all the public channel messages although, as discussed later, she cannot change their content. The key distribution process is illustrated schematically in figure 4. Alice begins by choosing a random bit sequence and for each bit randomly selects either the linear or the circular representation. She then prepares a regular-clocked sequence of photons in the appropriate polarization states and transmits them to Bob over the quantum channel. For the example shown in the figure Alice has chosen to send a one in the first timeslot using the linear representation i.e. a vertically polarized photon, a one in the second timeslot using the circular representation i.e. a right polarized photon, and so on. At the other end of the channel Bob makes an independent random choice of whether to perform a linear or a circular measurement in each time period and records the result. As discussed in the example above, the type of measurement is selected by applying a 1/4-wave retardation before the polarizer for circular and no retardation for linear, and the result depends on which of the detectors registers the photon. The optical transmission system will also inevitably suffer from a variety of loss processes that randomly delete photons from the system and in these cases neither of Bob's detectors fires and he denotes this null event by an 'X'. In the timeslots where Bob did receive a photon and happened to choose the same representation as Alice (as in timeslot 1, for example) the bit that he registers agrees with what Alice sent. In timeslots where Bob used a different representation to Alice (as in time-slot 2, for example) the outcome of the measurement is unpredictable and he is equally likely to obtain a one or a zero.

Alice and Bob now carry out a discussion using the classical public channel that enables them to generate a shared random bit sequence from the data and test its secrecy. Bob announces the timeslots when he received a photon and the *type* of measurement he performed in each but, crucially, not the *result* of the measurement as this would give away the bit value if Eve were monitoring the discussion. In the case of the transmission shown in figure 4 Bob reveals that he received photons in timeslots 1, 2, 6 and 8 using linear, and timeslots 3 and 5 using circular. Alice then tells Bob in which of these timeslots they both used the same representation (1, 3 and 8) and they discard all other data. In this way they identify the photons for which Bob's measurements had deterministic outcomes and hence distil the shared subset 101 from Alice's initial random bit sequence. This is the 'raw' key data. In practice, the process would of course be continued until a much longer sequence had been established.

Why do Alice and Bob go through this tedious and inefficient process? Recall that the goal is to establish a secret random bit sequence for use as a cryptographic key. Consider the situation illustrated in Fig 5 where Eve attempts to intercept the quantum transmission, make a copy, and then resend it on to Bob. In each timeslot Eve (like Bob) has to make a choice of what measurement to perform. Without any aprioi knowledge of the representation chosen by Alice, Eve (like Bob) has a 50% chance of performing an incompatible measurement as shown in the figure. This leads to a random outcome and a change of polariza-

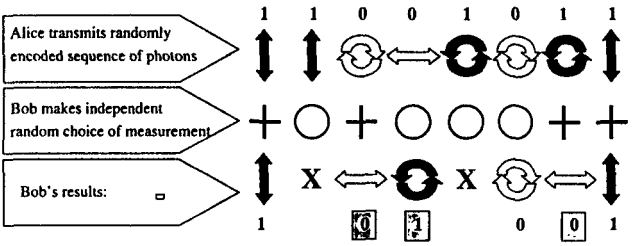

Fig. 4. Schematic representation of the quantum transmission phase of the BB84 quantum cryptography protocol. The top row shows Alice's outputs in 8 time slots that run sequentially from right to left. Bob's choice of measurements (cross=linear, circle =circular) and his results for the 8 timeslots are shown in the lower rows (X=no photon detected). During the public discussion Alice and Bob agree to discard the results where they used different representations (greyed boxes) and retain the shared bit sequence 101.

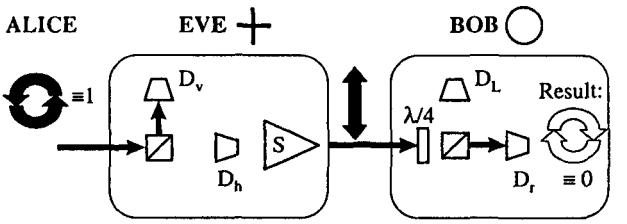

Fig. 5. Eve tries to intercept, make a copy, and then resend the bit sequence on to Bob. For each photon Eve has a 50% chance of choosing an incompatible measurement that leads to a random outcome. This is the case shown here where Eve has chosen to perform a linear measurement on Alice's circular photon. As a result Eve uses her source S to send on a vertical photon to Bob who now has a 50% chance of obtaining an error even though he has performed a compatible (as far as Alice and Bob are concerned) measurement.

tion state for the photon (note that we assume for simplicity that Eve makes the same type of polarization measurements as Bob, but the system is designed to be secure for any measurements that Eve may make). Eve has no way of knowing that she has performed an incompatible measurement because, unlike Bob, she does not have the benefit of the post transmission public discussion. The latter only takes place after the photons have arrived at Bob's end of the channel. Consequently, Eve sends a repolarized photon on to Bob who now has a 50% chance of observing an error in a timeslot where he has used the same representation as Alice and therefore expects a deterministic outcome. Consequently, if Eve makes continuous measurements on the channel she will generate a substantial bit-error rate of the order of 25% in the raw key. Of course, Eve may make measurements on only some of the photons or she may use other measurement techniques that yield less information but produce less disturbance on the channel [4, 15, 16]. Nevertheless, the crucial point is that Eve can only reduce the disturbance that she causes by also reducing the amount of information that she obtains; quantum mechanics ensures that these two quantities are directly related. For the specific example given above, Eve has a 50% chance per interception of making the correct choice of measurement and hence obtaining the correct bit and a 50% chance of making an incorrect choice of measurement that yields no information and causes disturbance on the channel. If Eve listens to the subsequent public discussion she can identify the instances in which her choice of measurement was correct and hence identify the bits (approximately 50%) in her data string that are shared with Alice and Bob. Hence if Eve intercepts 20% of the photons, for example, she will learn 10% of Alice and Bob's bits and generate an error-rate of around 5%. This simple example is unrealistic, because it does not describe all the measurement strategies that are available to Eve in a practical system, or the relative 'values' of the different types of information that she can obtain. Nevertheless, it does emphasise the basic principle of the technique which is that Alice and Bob can set an upper limit on the amount of information that Eve has obtained on their shared bit string simply by evaluating the error rate for their transmission [4]. As discussed below, if this is sufficiently low, they can generate a final highly secret key, if not they identify that the channel is currently insecure and cannot be used for secure key distribution. Quantum cryptography thus prevents the situation, which can always arise in principle with any classical key distribution system, where Alice and Bob's encrypted communications are compromised because they are unaware that Eve has surreptitiously obtained a copy of the key.

A full discussion of the final stages of the protocol that achieve this goal is beyond the scope of this paper, however, the main procedures that are involved will be briefly outlined. After discarding the inconclusive results from their bit strings, Alice and Bob publicly compare the parities of blocks of their data, and where these do not match, performing a bisective search within the block to identify and discard the error [4]. In this way they can derive a shared, error free, random bit sequence from their raw data together with a measurement of the error rate. This is achieved at the cost of leaking some additional information to

Eve in the form of the parities of the data subsets. In real systems transmission errors occur even when no eavesdropper is present on the channel. These errors can arise, for example, from the finite polarization extinction ratios of the various optical components in the system or from noise sources such as detector dark counts. In principle there is no way in to distinguish these errors from those caused by eavesdropping, hence all errors are conservatively assumed to have been generated by Eve. If the error rate is sufficiently low (typically of the order of a few percent in practice), then a technique known as 'privacy amplification' [17, 18] can be employed to distil from the error-corrected (but possibly only partially secret) key a smaller amount of highly secret key about which Eve is very unlikely to know even one bit. If, for example, Alice and Bob calculate that Eve may know e bits of their error-corrected n-bit string, they can generate from this data a highly secret m-bit key (where m(n-e) simply by computing (but not announcing as in error-correction) the parities of m publicly agreed-on random subsets of their data [4, 17, 18]. The final stage of the process is for Alice and Bob to authenticate their public channel discussions using an information-theoretically secure authentication scheme [19]. This is to prevent the powerful attack in which Eve breaks in to the public channel and impersonates Bob to Alice and visa-versa [4]. If this were possible Eve could share one key with Alice and another with Bob who would be unaware that this were the case. Like the one-time pad cipher, the authentication scheme requires Alice and Bob to possess in advance a modest amount of shared secret key data, part of which is used up each time a message is authenticated. However, this initial key is only required at system turn-on time because each implementation of the quantum key distribution protocol generates a fresh volume of key data some of which can be used for authentication. After privacy amplification and authentication Alice and Bob are now in possession of a shared key that is certifiably secret. They can now safely use this key together with an appropriate algorithm for data encryption purposes.

4 Conclusions

In the accompanying talk I will demonstrate how the theoretical ideas discussed above can be implemented and tested in a number of scenarios of real practical interest. In particular I will describe a scheme based on photon interference that we have developed over the last few years at BT [7, 20–24]. This system operates in the 1.3μm-wavelength fiber transparency window over point-to-point links up to ~50km in length [23] and on multi-user optical networks [6, 25]. I will also discuss how this technology performs on fiber links installed in BT's public network and discuss issues such as cross-talk with conventional data channels propagating at different wavelengths in the same fiber [24]. The experiments demonstrate that quantum cryptography can provide, at least from a technical point of view, a practical solution for secure key distribution on optical fiber links and networks. In summary, quantum cryptography has now moved a long way

from the original fascinating theoretical concept towards practical applications in optical communication systems.

Acknowledgements I would especially like to thank Keith Blow for his continued advice, support and encouragement and Simon Phoenix for his theoretical contributions. I would also like to acknowledge the important contributions of two graduate students, Christophe Marand and Guilhem Ensuque, to the experimental work mentioned above.

References

1. C. H. Bennett, 'Quantum information and computation', *Physics Today*, October (1995), for a review of this topic.
2. W. K. Wootters and W. H. Zurek, 'A single quantum cannot be cloned', *Nature*, **299** 802-803 (1982)
3. C. H. Bennett and G. Brassard, 'Quantum cryptography: public-key distribution and coin tossing', in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 175-179 (1984).
4. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, 'Experimental quantum cryptography', *Journal of Cryptology*, **5** 3-28 (1992).
5. A. K. Ekert, 'Quantum cryptography based on Bell's Theorem', *Physical Review Letters*, **67** 661-663 (1991)
6. P. D. Townsend, 'Quantum cryptography on multi-user optical fiber networks', *Nature*, **385**, 47-49 (1997)
7. C. Marand and P. D. Townsend, 'Quantum key distribution over distances as long as 30km', *Optics Letters*, **20** 1695-1697 (1995)
8. J. D. Franson and B. C. Jacobs, 'Operational system for quantum cryptography', *Electronics Letters*, **31** 232-234 (1995)
9. R. J. Hughes, G. G. Luther, G. L. Morgan and C. Simmons, 'Quantum cryptography over 14km of installed optical fiber', *Proc. 7th Rochester Conf. on Coherence and Quantum Optics (eds J. H. Eberly, L. Mandel and E. Wolf)*, 103-112 (Plenum, New York, 1996)
10. H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, 'Interferometry with Faraday mirrors for quantum cryptography', *Electronics Letters*, **33**, 586-587 (1997)
11. G. S. Vernam, *J. Amer. Inst. Electr. Engrs.*, **45**, 109-115 (1926)
12. C. E. Shannon, 'Communication theory of secrecy systems', *Bell Syst. Tech. J.*, **28**, 656-715 (1949)
13. H. Beker and F. Piper, Cipher Systems : *the Protection of Communications*, (Northwood Publications, London, 1982). See also G. Brassard, Modern *Cryptology, Lecture Notes in Computer Science*, eds G. Goos and J. Hartmanis (Springer-Verlag, Berlin, 1988)
14. P Shor, 'Algorithms for quantum computation: Discrete logarithm and factoring', Proc. 35th *Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society Press, 1994), 124-134
15. A. K. Ekert, B. Huttner, G. M. Palma and A. Peres, 'Eavesdropping on quantum cryptosystems', *Physical Review A* **50**, 1047-1056 (1994)
16. B. Huttner and A. K. Ekert, 'Information gain in quantum eavesdropping', *J. Mod. Opt.*, **41**, 2455-2466 (1994)

17. C. H. Bennett, G. Brassard and J.-M. Robert, 'Privacy amplification by public discussion', *SIAM Journal on Computing*, **17** 210-229 (1988).
18. C. H. Bennett, G. Brassard, C. Crepeau and U. Maurer, 'Generalized privacy amplification', *SIAM Journal on Computing*, **17** 210-229 (1988).
19. M. N. Wegman and J. L. Carter, 'New hash functions and their use in authentication and set equality', *J. Computer and System Sciences*, **22**, 265-279 (1981)
20. P. D. Townsend, J. G. Rarity and P. R. Tapster, 'Single-photon interference in a 10km long optical fiber interferometer', *Electronics Letters*, **29** 634-635 (1993)
21. P. D. Townsend, 'Secure key distribution system based on quantum cryptography', *Electronics Letters*, **30** 809-810 (1994)
22. S. J. D. Phoenix and P. D. Townsend, 'Quantum cryptography: how to beat the code breakers using quantum mechanics', *Contemporary Physics*, **36** 165-195 (1995)
23. P. D. Townsend, 'Quantum cryptography on optical fiber networks', *Optical Fiber Technology*, (In Press)
24. P. D. Townsend, 'Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength division multiplexing', *Electronics Letters*, **33** 188-189 (1997)
25. P. D. Townsend, S. J. D. Phoenix, K. J. Blow and S. M. Barnett, 'Design of quantum cryptography systems for passive optical networks', Electronics Letters, **30** 1875-1877 (1994). See also S. J. D. Phoenix, S. M. Barnett, P. D. Townsend and K. J. Blow, 'Multi-user quantum cryptography on optical networks', *Journal of Modern Optics*, **42**, 1155-1163 (1995) 18 19