PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A
MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

The Principles of Quantum Cryptography

Stephen M. Barnett and Simon J. D. Phoenix

Phil. Trans. R. Soc. Lond. A 1996 **354**, 793-803
doi: 10.1098/rsta.1996.0032

The principles of quantum cryptography

By Stephen M. Barnett[1] and Simon J. D. Phoenix[2]

[1] *Department of Physics and Applied Physics, University of Strathclyde, Glasgow G4 0NG, UK*

[2] *BT Laboratories, Martlesham Heath, Ipswich IP5 7RE, UK*

Two parties can communicate in secret if they already share a sufficient quantity of secret information. The problem then is how to distribute this secret information or key. Quantum cryptography provides the potential to ensure the security of the process of key distribution and hence to guarantee the covert nature of the communication. The security of quantum key distribution relies on the principles of quantum theory and its successful implementation requires the development of quantum optical techniques.

1. Introduction

Coded messages are as old as the desire to keep secrets. Secrecy has been achieved by the expedient of keeping the very existence of the message secret or by disguising it so as to obscure its meaning. In either case the secrecy relies on some information denied to any possible eavesdropper attempting to intercept the message; the intended recipient needs to know of the existence of a hidden message and where to find it, or the key to unlock the meaning from a coded message. It is not always convenient or even possible to hide the existence of a message and so we need to consider the problem of obscuring the meaning by encoding the message in the form of a cipher. This takes the message or plaintext and converts it into a ciphertext or cryptogram for transmission. Quantum cryptography (Wiesner 1983; Bennett & Brassard 1984; Bennett *et al.* 1992*a*) provides a radically new solution to this age-old problem by exploiting the quantum nature of light to protect the transmission of information against interception by an eavesdropper.

One of the oldest and simplest of all codes is the transposition, or Caesarean, cipher (attributed to Julius Caesar), in which the letters of the message are shifted a known (and secret) number of places in the alphabet. However, the resulting cipher is not very secure. Consider for example the cipher YORQRP EXP X HKFCB. The message may be decoded by simply trying all 25 possible displacements between the message and cipher alphabets and seeing which of them leads to a sensible message. In this case we find that shifting the cipher alphabet 23 places so that A becomes X, B becomes Y, and so on, leads to the message BRUTUS HAS A KNIFE. Other possible texts are meaningless in English. This method of encoding or encrypting the message is insecure because of the strictly limited number of possible ways in which the message could have been encoded. Another simple cipher is the substitution code, in which each letter is replaced by a symbol so that the message is replaced by a sequence of symbols. In principle, each of the symbols could represent any of the

Printed in Great Britain

TEX Paper

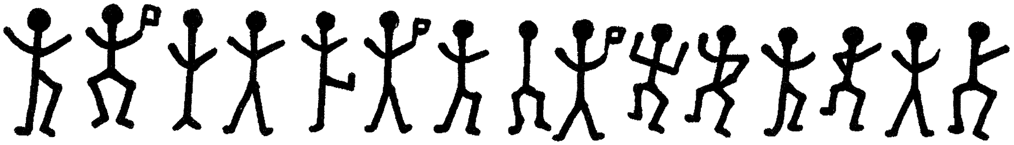

Figure 1. The first coded message to appear in 'The Adventure of the Dancing Men'. (After Conan Doyle 1903.)

letters and such a code might seem secure but it is not. Consider, for example, the string of symbols in figure 1. These are the first of a series of mysterious messages that appeared to challenge Sherlock Holmes in one his cases (Conan Doyle 1903). The method of deciphering this type of code relies on the frequency with which symbols arise and, given a sufficiently long string, the code can be broken. As Holmes explains:

> The first message submitted to me was so short that it was impossible for me to do more than say with some confidence that the (fourth) symbol stood for E. As you are aware, E is the most common letter in the English alphabet, and it predominates to so marked an extent that even in a short sentence one would expect to find it most often. Out of the 15 symbols in the first message four were the same, so it was reasonable to set this down as E. It is true that in some cases the figure was bearing a flag and in some cases not, but it was probable from the way in which the flags were distributed that they were used to break the sentence into words.

Subsequent messages, together with a knowledge of English, allowed Holmes to break the code.

Codes of the type just described are easily deciphered because the amount of secret information applied in producing the cipher is too little; in particular, each letter from the message always appears in the same form in the cipher. More sophisticated cipher systems require more secret information; indeed the only fully secure way to communicate is with an equal quantity of secret (key) information as that forming the message to be sent and to use this key only once (Shannon 1949). The simplest cipher system to guarantee secrecy in this way is the one-time pad (Vernam 1926; Chambers 1985). We can send an N-letter plaintext message m in perfect secrecy with the aid of a random N-letter string k by adding this (modulo the alphabet size) letter by letter to the message to obtain the ciphertext c for transmission. The ciphertext will be secure because, being formed by the sum of the message and a random string, it is itself a random string of symbols. Anyone intercepting such a message and not having access to the key will know that the message exists and how long it is (although even this can be disguised), but will only be able to guess at its meaning. The only way to regain m from c is to have a copy of the key k and to subtract k from c (modulo the alphabet size). Crucial to the absolute secrecy of the one-time pad is that it should only be used once and, if method is to form the basis of a secure communication system, then provision needs to be made for the distribution and storage of vast amounts of key data.

In practice, a high level of security, although less than the theoretically possible perfect secrecy, is available through cipher systems working with keys that are significantly shorter than the encoded message. The best known of these is the data encryption standard (DES), which uses a key of 56 bits and a publicly known algorithm to encrypt the input plaintext to generate the required ciphertext (Beker & Piper 1982; Denning 1982; Brassard 1988). In principle, DES is vulnerable to the same

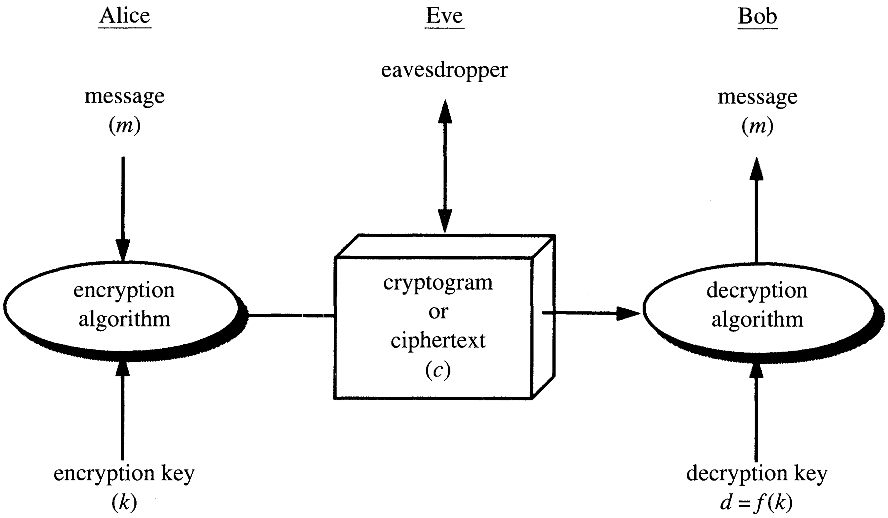

Figure 2. The basic elements of a cipher system. Alice employs a known algorithm to produce a ciphertext (c) from a message (m) and a key (k). Bob can reproduce the original message with the use of the decryption key (d). The decryption key need not be the same as the encryption key but it should be easily derivable from it.

sort of exhaustive key search as the transposition code, but we can get an idea of the scale of the practical problem by considering the number of possible keys. In the transposition code there are 25 possible keys, one for each possible shift between the plaintext and ciphertext alphabets. This number of keys pales in comparison with the 2^{56} or about 7×10^{16} of possible keys in DES. For a computer able to check 10^6 keys per second, an exhaustive key search on a DES-encrypted ciphertext might take up to 2000 years! There are more sophisticated cryptanalytic techniques than simply checking all possible keys, but a practical algorithm for breaking DES has yet to be demonstrated.

Figure 2 summarizes the operations involved in the cryptographic protection of a communication channel. The transmitter 'Alice' wishes to send a secret message to the receiver 'Bob' without revealing any information to 'Eve', an unauthorized eavesdropper. The plaintext message m is encoded using the secret key k to form a ciphertext c which is transmitted to Bob who can decipher the ciphertext using the same key. All of this presupposes the existence of the vital shared secret key held by Alice and Bob but denied to Eve. It follows that Alice and Bob require a second, very secure, communication channel in order to distribute the key. The ultimate security of the cryptographic system relies on this second channel being protected from eavesdropping. This potential loophole in key distribution has motivated the development of public-key cryptosystems (Diffie & Hellman 1976) and quantum cryptography.

Quantum cryptography is the application of principles from quantum theory to the problem of secure communications. The fundamental principle upon which it relies is that, in quantum physics, measurements induce a change in the system under scrutiny. Any unauthorized eavesdropper on a communication channel will be bound by this principle and, in attempting to gain information about the message sent, will leave the signs of their interference by modifying the states of the bits forming the message. By open discussion of some of the data sent and received, the two legitimate users of the channel can infer whether anyone has been listening in and hence decide if their data, the secret key, is secure. A number of introductions to quantum cryptography have been published, the most recent of these being by Phoenix & Townsend (1995) and Hughes (1995).

2. Quantum information

Quantum cryptography is possible because there exist in quantum physics some elements without analogue in the classical domain. Most fundamental among these is the superposition principle for probability amplitudes. This contains within it the idea that amplitudes for phenomena that are in principle indistinguishable add coherently and that it is the modulus squared of the sum of such amplitudes that determines the probability of occurrence for a possible outcome. The superposition principle carries with it other non-classical features, most notably the incompatibility of certain observable quantities and the non-local properties of entangled states. It is the impossibility of obtaining fully accurate information about incompatible observables that protects quantum cryptographic systems from eavesdropping. In order to appreciate the principles underlying quantum cryptography, we begin by examining the way in which information can be encoded on a quantum system.

The simplest non-trivial quantum system is the two-state system, examples of which include the polarization of a photon, the choice of two possible trajectories of a particle and the orientation of the spin associated with a spin-half particle. Such two-state systems provide a physical representation of the quantum binary digit (Deutsch 1989). We can encode information on a quantum binary digit by associating the value 0 with one possible state (which we denote $|0\rangle$) and the value 1 with the state ($|1\rangle$), which is orthogonal to it. Measurement of an observable having these states as eigenstates allows us to distinguish between them and to recover the bit of information. This is the same idea as that encountered in the classical domain. Where quantum bits differ from their classical counterparts is that it is possible to have states formed by superposition of the states $|0\rangle$ and $|1\rangle$ in the form $a_0|0\rangle + a_1|1\rangle$ (with a_0 and a_1 being complex numbers). A superposition state will be an eigenstate of a different and complementary observable to that associated with the states $|0\rangle$ and $|1\rangle$. We will be able to obtain the information encoded in a quantum bit only if we know which basis of orthogonal states has been used and therefore which of the possible observable quantities we have to measure.

Consider, for example, a stream of single photons, each of which is prepared with either vertical or horizontal polarization. We denote these states by the kets $|V\rangle$ and $|H\rangle$, respectively, and we associate vertically polarized photons with the value 1 and horizontally polarized photons with the value 0. A carefully oriented polarizer will allow us to distinguish between the states $|V\rangle$ and $|H\rangle$. However, a polarizer oriented at an angle θ to the vertical provides a means of distinguishing states $|V'\rangle$ and $|H'\rangle$ related to $|V\rangle$ and $|H\rangle$ by

$$|V'\rangle = \cos\theta|V\rangle + \sin\theta|H\rangle, \quad |H'\rangle = \cos\theta|H\rangle - \sin\theta|V\rangle. \tag{2.1}$$

A measurement of the polarization of a photon prepared in the state $|V\rangle$ using the rotated orientation will find the polarization state to be $|V'\rangle$, and hence assign the correct value of 1, with probability $\cos^2\theta$. It will find the polarization to be $|H\rangle$ and assign the incorrect value of 0 with probability $\sin^2\theta$. Clearly, if $\theta = 0$ then ideally there will be no error in recovering the information, while if $\theta = \frac{1}{2}\theta$ there will be a 100% error rate! Although a 100% error rate sounds alarming, it is, of course, easily dealt with by a simple bit-flip; replacing every 0 by a 1 and vice versa will reproduce the original message. The worst situation occurs when $\theta = \frac{1}{4}\theta$ and there is a 50% chance of error. This leads to a random string of results that is completely independent of the original signal and hence contains no information.

The act of measurement will modify the state of a system and hence will affect the results of any further measurements that might be made. In practice, the measurement of the photon polarization involves the absorption and therefore destruction of the photons. The information gained in performing the measurement could be used to prepare a replacement photon, but the act of measurement and regeneration will not, in general, produce a copy of the original (Wootters & Zurek 1982). Unless the original photon was in an eigenstate of the observable we chose to measure, we would have insufficient information to make an accurate copy.

In the following discussion of the quantum key distribution, based on the Bennett–Brassard protocol (Bennett & Brassard 1984), we will consider photons prepared in either one of two states of linear polarization ($|V\rangle$ or $|H\rangle$) or in the state of left ($|L\rangle$) or right ($|R\rangle$) circular polarization. The two possible states of circular polarization may be written as superpositions of the states of linear polarization:

$$|L\rangle = \frac{1}{\sqrt{2}}\{|V\rangle + \mathrm{i}|H\rangle\}, \quad |R\rangle = \frac{1}{\sqrt{2}}\{|V\rangle - \mathrm{i}|H\rangle\}. \tag{2.2}$$

Measurement of the linear polarization associated with a photon prepared in a circularly polarized state will lead to either of the possible results with equal probability, as will measurement of the circular polarization associated with a linearly polarized photon. The situation is more subtle than it appears at first sight; not only do we obtain a probabilistic result when measuring the 'wrong' polarization, but we have no indication that we have in fact measured the wrong observable. All that we have is the result of one polarization measurement.

Consider what will happen if Alice transmits a photon in a chosen state of circular polarization to Bob, who then performs a measurement of the circular polarization. In the absence of any intervention by an eavesdropper (Eve), the result of Bob's measurement should tally with the choice of state made by Alice. If Eve makes a measurement of circular polarization and then prepares and retransmits a replacement circularly polarized photon then Bob's measurement will provide the same result and all three characters will be in possession of the same bit of information. Moreover, Alice and Bob will be unaware that Eve has been listening in. If, as depicted in figure 3, Eve makes a measurement of the linear polarization of the photon then her measurement provides no information about the bit sent by Alice; she will infer the correct bit value with a probability of one half, but this is no better than simply guessing the bit. If she retransmits a replacement linearly polarized photon then Bob's measurement of the state of circular polarization will produce either left or right circular polarization with equal probability. In other words, Eve's measurement of the wrong observable and subsequent retransmission will induce an error in Bob's measurements with a probability of one half. These errors take the form of disagreements between the bit chosen by Alice and that inferred by Bob from his measurement. The remaining problem is to devise a method whereby Eve, by the action of eavesdropping, is forced to induce errors and thereby reveal the fact that she has been listening in. The sequence of operations leading to either the detection of Eve or the establishment of a secret key known only to Alice and Bob is referred to as a protocol.

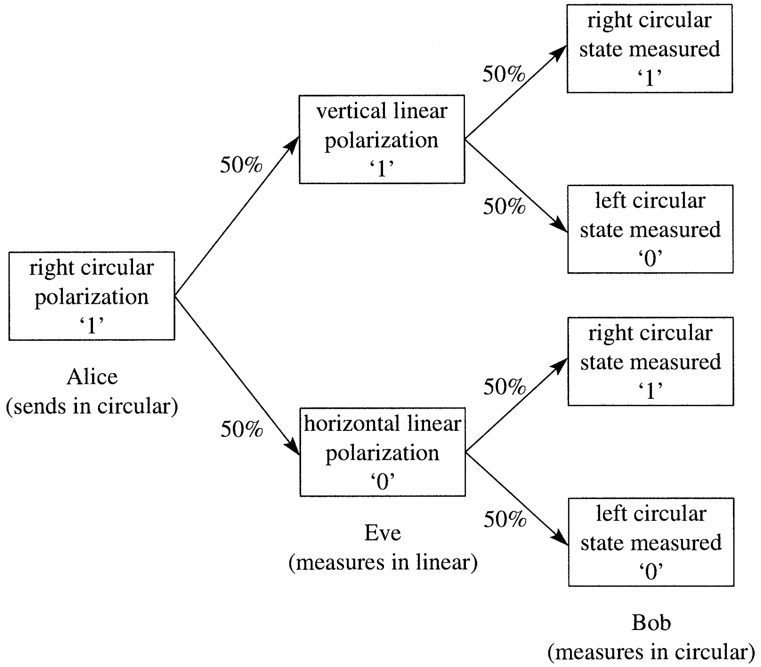

Figure 3. Eve's measurement of the wrong observable will induce an error with a probability of one half in Bob's measurements. (After Phoenix & Townsend 1993.)

3. Quantum key distribution

The first complete protocol for the distribution of a key by quantum cryptography was devised by Bennett & Brassard (1984) and is now referred to as BB84. A description of its operation will serve to illustrate the principles underlying all such protocols.

Alice generates a random sequence of zeros and ones and encodes them on the polarizations of individual photons. A one is either represented as a state of right circular polarization or as a state of vertical polarization and a zero is encoded as left circular or horizontal linear polarization. The choice of linear or circular polarization is also made at random. For the purposes of the present discussion we will assume that the photons are generated in a regular sequence so that exactly one photon is present in each of the time slots. Bob receives this sequence of photons and chooses, randomly and *independently* of Alice, whether to measure the circular or linear polarization for each photon. This procedure is depicted in figure 4, where an example sequence of 14 bits is shown with the coding chosen by Alice. Bob's choices of measurement basis (circular or linear polarization) together with the bit values are inferred by Bob from his observations. We can see that one of three things can happen; Bob does not detect a photon, or if he does he either measures in the same basis or the alternative basis to that used by Alice. At this point Alice and Bob engage in public discussion and exchange information about which basis (although not which of the two basis states) was used for each time slot, that is they disclose whether circular or linear polarization was used to prepare and measure each photon. Those instances where Alice and Bob have used different bases are discarded as no correlation between sent and received data is expected. They also discard those time slots where no photon was detected by Bob. This results in the loss of about one half of the time slots where

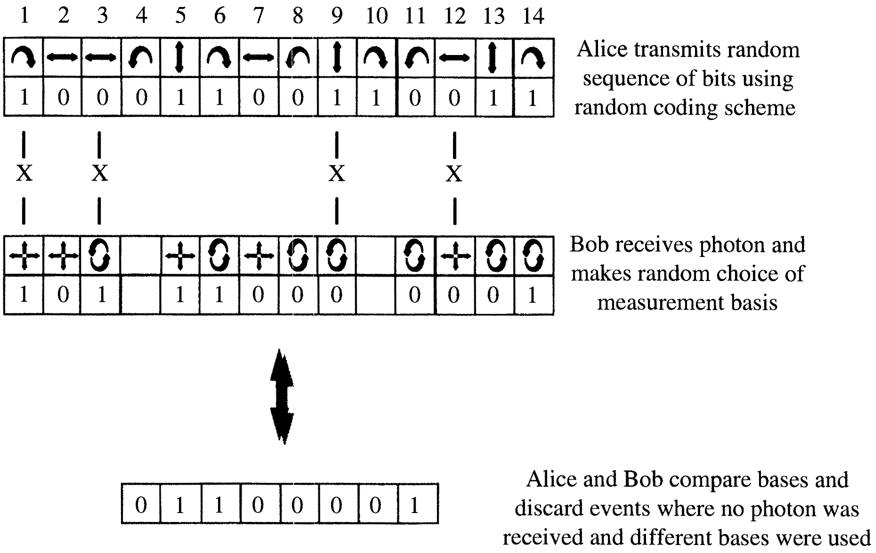
1 2 3 4 5 6 7 8 9 10 11 12 13 14
1 0 0 0 1 1 0 0 1 1 0 0 1 1
Alice transmits random sequence of bits using random coding scheme
X X X X
1 0 1 1 1 0 0 0 0 0 0 1
Bob receives photon and makes random choice of measurement basis
0 1 1 0 0 0 0 1
Alice and Bob compare bases and discard events where no photon was received and different bases were used

Figure 4. An example of 14 time slots in the transmission between Alice and Bob. In the slots marked with an X, Bob measures the wrong basis. In slots 4 and 10 he fails to detect any photon. In the absence of an eavesdropper, the remaining time slots represent shared key data.

Bob detected a photon. At this stage Alice and Bob have bits corresponding to those instances where they have used the same basis. If the channel is secure they should now be in possession of an identical sequence of random bits. The random choice of bases by both Alice and Bob is crucial to the security because any eavesdropper, and indeed Bob himself, must guess the correct basis in order to receive a key bit.

If an eavesdropper (Eve) has been listening in, then she has the problem that, at the time she is able to make a measurement, she is unaware of the correct observable to measure in order to extract the information. Her only option is to make a measurement and then to send a replacement photon to Bob, but she will have to guess which basis to measure and, like Bob, she will only guess correctly on about one half of the occasions. On those occasions when she chooses the same basis the photon she transmits to Bob will be a faithful copy of that received from Alice. However, as described at the end of the preceding section, if she measures in the wrong basis then the result of Bob's measurement will coincide with the value transmitted by Alice only half of the time. Hence, Eve's intervention will induce a discrepancy between Alice's and Bob's bit sequence with a probability of $\frac{1}{4}$. If Alice and Bob have a sequence of N bits where they used the same basis, and therefore expect to have N identical bits, the probability that there will be no errors in this data if Eve has attempted to eavesdrop will be $(\frac{3}{4})^N$. Alice and Bob check for the presence of Eve by publicly disclosing the bit values associated with a subset of those remaining time slots where they used the same bases. If all of the bits coincide then they can be confident that no eavesdropper has been active and that the remaining undisclosed bits form a secret key known only to them.

The first experimental demonstration of this protocol (Bennett *et al.* 1992) is shown schematically in figure 5. The light was in the form of very faint flashes from a green LED transmitted over a distance of approximately 30 cm. Each pulse of light contained an average of 0.1 photons. By randomly switching the voltage drive on her Pockel's cell for each pulse, Alice could randomly select one of the four polarization states ($|V\rangle$, $|H\rangle$, $|L\rangle$ or $|R\rangle$). Bob's apparatus consisted of a second independently

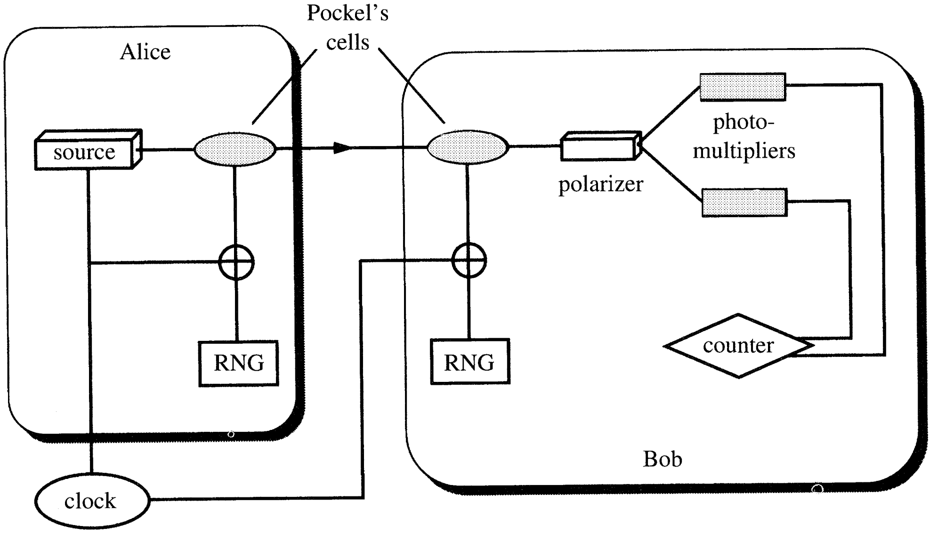

Figure 5. Schematic of the elements employed in the first implementation of the BB84 protocol, where RNG denotes a random number generator.

switched Pockel's cell followed by a calcite crystal and detectors to determine either the linear or circular polarization of each photon. This demonstration experiment realized a secure key comprising 105 bits in a transmission of about 10 min duration. More realistic prototypes and demonstration experiments have been performed using optical fibres resulting in key distribution over distances of tens of kilometres (Townsend *et al.* 1993*a*, *b*; Muller *et al.* 1993; Townsend & Thompson 1994; Townsend 1994; Franson & Ilves 1994*a*, *b*; Hughes 1995). A discussion of quantum cryptographic key distribution using optical fibres is given in the accompanying paper by Townsend (this volume). All realistic systems suffer from noise and this will induce a number of discrepancies between Alice's and Bob's data even in the absence of Eve. The only safe way to proceed is to assume that these arise due to the intervention of Eve. If the error rate is sufficiently low then further public discussion between Alice and Bob allows them to correct any errors in their key data and to obtain a secret key as a subset of their raw key data. This process is known as privacy amplification (Bennett *et al.* 1988). The problem is further complicated by the fact that the required public discussion between Alice and Bob reveals useful information to Eve about the data she has obtained (Huttner & Ekert 1994).

It is worth emphasizing the importance of there being no more than a single photon in any given time slot. If there were two photons then a resourceful Eve could separate them and measure the circular polarization associated with one of them and the linear polarization of the other. This is the reason for using low-intensity pulses of light; in the experiment of Bennett *et al.* (1992*a*) only one in ten pulses actually contains a photon and only about one in a hundred has two or more. She cannot make true copies of a single photon as to do so would violate the superposition principle (Wootters & Zurek 1982).

Eve is not limited to simply measuring the same observables as those used by Alice and Bob. She may, for example, measure an observable intermediate between those chosen by them corresponding, in the protocol described above, to measuring components of elliptical polarization (Bennett *et al.* 1982; Phoenix 1993). However, there is no strategy open to Eve which will allow her to both obtain the key and escape detection by Alice and Bob.

4. Other protocols

Quantum cryptography relies on principles of quantum physics governing the measurements made by Eve and Bob. The BB84 protocol relies for its security on the principle that measurements by Eve will inevitably lead to the introduction of discrepancies between the data recorded by Alice and Bob on those occasions where they used the same bases. The remaining data recorded in those time slots when they used different bases is discarded or rejected. However, this data can also tell us something about the activity of a possible eavesdropper (Barnett & Phoenix 1993*a*). So called rejected-data protocols have been developed to take advantage of all of the data shared by Alice and Bob (Barnett & Phoenix 1993*a*, *b*; Barnett *et al.* 1993). The idea is to use the measured statistics of the results in those time slots when Alice and Bob used different bases. A rejected-data protocol is designed so that the action of Eve will lead to a significant change in these statistics compared to that expected if Eve were not listening in. These protocols require the use of no less than three different bases by Alice and Bob. This follows from the idea that a necessary condition for Eve to be detected is that she uses a different basis to both Alice and Bob (Blow & Phoenix 1993). In a rejected-data protocol using only two different bases, Eve could always escape detection by measuring either of the observables used by Alice and Bob.

It is by no means necessary to use both of the states associated with a given basis. The minimum requirement for a secure quantum cryptographic channel is to use two non-orthogonal states (Bennett 1992). Two state protocols can be implemented interferometrically and efforts are being made by Marand & Townsend at BT and by Hughes at Los Alamos to develop prototype systems.

A radically different approach to quantum cryptography is to use the correlations between pairs of entangled photons produced in parametric down-conversion (Ekert 1992). The correlations are non-local in that they violate Bell's inequality, which is derived from the idea of local realism (Bell 1987). Hence, observation of the failure of this inequality is at odds with the concept of local realism. The action of an eavesdropper will introduce an element of local reality as she has established the value associated with the result of her measurement. This restores Bell's inequality and, in doing so, provides Alice and Bob with the means to detect her. Further developments have shown that an exactly equivalent degree of security can be achieved with single particles (Bennett *et al.* 1992*b*; Barnett & Phoenix 1993*b*).

Other protocols have been proposed but all of them have in common that Alice and Bob compare their data, in effect, performing a quantum experiment. Departures from the expected behaviour are used to identify the presence of an eavesdropper.

5. Conclusions

Quantum cryptography has developed in a short space of time from little more than a curiosity into a near practical technology. In contrast to more conventional methods, it relies on physical principles for its success. Put simply, if quantum mechanics is correct then quantum cryptography provides a method for secure key distribution. It is an intriguing thought that the ultimate limit on our confidence in a quantum cryptographic device might be our confidence in the correctness of quantum mechanics, or, more precisely, of those features of quantum mechanics upon which the security depends.

Our interest in and work on quantum cryptography has benefited greatly from the interaction with Keith Blow, Bruno Huttner, Rodney Loudon, Norbert Lütkenhaus and Paul Townsend.

References

Barnett, S. M. & Phoenix, S. J. D. 1993*a* Information-theoretic limits to quantum cryptography. *Phys. Rev.* A **48**, R5–R8.

Barnett, S. M. & Phoenix, S. J. D. 1993*b* Bell's inequality and rejected-data protocols for quantum cryptography. *J. Mod. Opt.* **40**, 1443–1448.

Barnett, S. M., Huttner, B. & Phoenix, S. J. D. 1993 Eavesdropping strategies and rejected-data protocols in quantum cryptography. *J. Mod. Opt.* **40**, 2501–2513.

Bekker, H. & Piper, F. 1982 *Cipher systems: the protection of communications.* London: Northwood Publications.

Bell, J. S. 1987 *Speakable and unspeakable in quantum mechanics.* Cambridge University Press.

Bennett, C. H. 1992 Quantum cryptography using any two non-orthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124.

Bennett, C. H., Brassard, G., Breidbart, S. & Wiesner, S. 1983 Quantum cryptography, or unforgetable subway tokens. In *Advances in Cryptology: Proc. Crypto 82*, pp. 267–275. New York: Plenum.

Bennett, C. H. & Brassard, G. 1984 Quantum cryptography: public-key distribution and coin tossing. In *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore), pp. 175–179.

Bennett, C. H., Brassard, G. & Mermin, N. D. 1992*b* Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557–559.

Bennett, C. H., Brassard, G. & Robert, J.-M. 1988 Privacy amplification by public discussion. *SIAM Jl Comput.* **17**, 210–229.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. 1992 Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28.

Blow, K. J. & Phoenix, S. J. D. 1993 On a fundamental theorem of quantum cryptography. *J. Mod. Opt.* **40**, 33–36.

Brassard, G. 1988 *Modern cryptology* (Lecture Notes in Computer Science) (ed. G. Goos & J. Hartmanis). Berlin: Springer.

Chambers, W. G. 1985 *Basics of communications and coding*, pp. 207–210. Oxford: Clarendon.

Conan Doyle, A. 1903 The Adventure of the Dancing Men. *The Strand Magazine* **26**, no. 156. (Reprinted 1989 *The original illustrated Sherlock Holmes* Secaucus: Castle.)

Denning, D. E. R. 1982 *Cryptography and data security.* Reading, MA: Addison-Wesley.

Deutsch, D. 1989 Quantum computational networks. *Proc. R. Soc. Lond.* A **425**, 73–90.

Diffie, W. & Hellman, M. E. 1976 New directions in cryptography. *IEEE Trans. Inf. Theory* **IT-22**, 644–654.

Ekert, A. K. 1992 Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663.

Franson, J. D. & Ilves, H. 1994*a* Quantum cryptography using optical fibres. *Appl. Opt.* **33**, 2949–2954.

Franson, J. D. & Ilves, H. 1994*a* Quantum cryptography using polarisation feedback. *J. Mod. Opt.* **41**, 2391–2396.

Hughes, R. J., Alde, D. M., Dyer, P., Luther, G. G., Morgan, G. L. & Schauer, M. 1995 Quantum cryptography. *Contemp. Phys.* **36**, 149–163.

Huttner, B. & Ekert, A. K. 1994 Information gain in quantum eavesdroping. *J. Mod. Opt.* **41**, 2455–2466.

Muller, A., Breguet, J. & Gisin, N. 1993 Experimental demonstration of quantum cryptography using polarised photons in optical fibre over more than 1 km. *Europhys. Lett.* **23**, 383–388.

Phoenix, S. J. D. 1993 Quantum cryptography without conjugate coding. *Phys. Rev.* A **28**, 96–102.

Phoenix, S. J. D. & Townsend, P. D. 1993 Quantum cryptography and secure optical communications. *BT Tech. Jl* **11**, 65–75.

Phoenix, S. J. D. & Townsend, P. D. 1995 Quantum cryptography—how to beat the codebreakers using quantum mechanics. *Contemp. Phys.* **36**, 165–195.

Shannon, C. E. 1949 Communication theory of secrecy systems. *Bell System Tech. Jl* **28**, 656–715.

Townsend, P. D. 1994 Secure key distribution based on quantum cryptography. *Electron. Lett.* **30**, 809–810.

Townsend, P. D., Rarity, J. G. & Tapster, P. R. 1993*a* Single-photon interference in a 10 km long optical fibre interferometer. *Electron. Lett.* **29**, 634–635.

Townsend, P. D., Rarity, J. G. & Tapster, P. R. 1993*b* Enhanced single-photon fringe visibility in a 10 km long quantum cryptography channel. *Electron. Lett.* **29**, 1292–1293.

Townsend, P. D. & Thompson, I. 1994 A quantum key distribution channel based on optical fibre. *J. Mod. Opt.* **41**, 2425–2434.

Vernam, G. S. 1926 Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elect. Engrs* **45**, 109–115.

Wiesner, S. 1983 Conjugate coding. *Sigact News* **15**, 78–88. (The original manuscript was written *ca.* 1970.)

Wootters, W. K. & Zurek, W. H. 1982 A single quantum cannot be cloned. *Nature* **299**, 802–803.