united nations
educational, scientific
and cultural
organization

international atomic
energy agency

the
abdus salam
international centre for theoretical physics

Winter College on Optics and Photonics
7 - 25 February 2000

1218-23

"Quantum Key Distribution"
(Reprints)

W.T. RHODES
Georgia Institute of Technology
USA

Please note: These are preliminary notes intended for internal distribution only.

Contemporary Physics, 1995, volume 36, number 3, pages 165–195

Quantum cryptography: how to beat the code breakers using quantum mechanics

SIMON J. D. PHOENIX and PAUL D. TOWNSEND

In a series of recent experiments a radical new technique has been demonstrated that could have far-reaching consequences for the way in which the confidentiality and integrity of our networks is protected. This technique, known as quantum cryptography, is the result of a synthesis of ideas from fundamental quantum physics and classical encryption and has lead to a radical new approach to the business of secure communications. We review the origins of and developments in this rapidly growing field and assess the current status of both the theory and the experiments.

1. Introduction

1.1. *Quantum cryptography: a practical reality*

In 1989 a collaboration between IBM and the University of Montreal performed an experiment that could have far-reaching consequences for the way in which we protect our most sensitive information on communications networks [1]. In essence, this deceptively simple experiment used single photons, and a clever protocol that exploited their quantum properties, to establish an identical random sequence of bits at two locations 30 cm apart. The transmission was performed in such a way that only the transmitter and the receiver could know this sequence. Because of the quantum properties any attempt at interception could be detected and rendered ineffective, thereby assuring the secrecy of the random bit string. The experiment demonstrated, in principle, how two people at remote locations can establish a secret and guarantee its secrecy. The technique, known as 'quantum cryptography' had become a practical reality. Ideas that had first arisen [2] early in the 1970s had now reached fruition and resulted in the remarkable IBM–Montreal experiment.

In the last few years, progress has been rapid and several experiments have now demonstrated the feasibility of quantum cryptography over a range of distances and wavelengths in optical fibre [3, 4] using readily available telecommunications components. A working prototype has been built at BT Laboratories to securely transmit information† over distances of up to 30 km in optical fibre using quantum cryptography [5–7]. This prototype exploits the properties of single photons at a wavelength of 1·3 μm using a phase coding scheme. Prototype quantum cryptography systems have also been developed to operate at shorter wavelengths using polarization coding schemes [3, 4, 8]. Distances of up to 1 km have been achieved with these systems. Although still very much a laboratory-based demonstrator requiring further work before commercial exploitation, quantum cryptography is a practical reality. These crucial experiments have shown [1, 3–9] that the processing of information at a quantum-mechanical level can lead to new and surprising developments that can find important applications in the business world of telecommunications.

A quantum cryptography system works because the world behaves in a quantum-mechanical way. Underpinning the achievements of the experiments are some remarkable theoretical features. Measurement in quantum mechanics occupies a central role; the role of measurement in quantum cryptography is central to the ability to provide guaranteed security. Complementarity is at the heart of the unique features of measurement in quantum mechanics and it is precisely this feature of quantum systems that is exploited to guarantee the security. Quantum cryptography works because quantum mechanics works and the design of such secure systems requires an appreciation of the subtleties involved in describing a quantum measurement process. Because information on quantum cryptography systems is carried on single photons, recovery of that information requires a quantum measurement process with all that this implies. It is remarkable that a technique so apparently abstract has grown from concept to near-application in such a short time.

This review paper will focus on some of the main issues that we have faced here at BT in our implementation of a

Authors address: BT Laboratories, Martlesham Heath, Ipswich IP5 7RE, UK.

†Strictly speaking the information transmitted forms the key for use in a cryptographic application. This distinction will be discussed in the next section.

0010-7514/95 $10.00 © 1995 Taylor & Francis Ltd.

practical quantum cryptography scheme. In the accompanying article in this issue, Richard Hughes describes the approach taken by his group at Los Alamos. We shall try to outline the major theoretical and experimental considerations that have arisen and give an overview of our current progress. We hope that this approach will allow a comprehensive account of our quest for a practical quantum cryptography system to emerge in greater depth and consistency than would otherwise have been the case. We shall see, however, that in fact even the simplest practical implementation of quantum cryptography addresses fundamental questions across a range of disciplines. We shall attempt to convey a flavour of our work in these areas and to given an insight into how we see the pieces of the jigsaw puzzle fitting together.

Our theoretical work has concentrated on developing general approaches both to quantum cryptography and to the examination of specific cases. The use of an information-theoretical approach has allowed a greater degree of generality and pointed to new concepts and tools. The aim is, of course, to set the limits for any practical scenario. Because the *raison d'être* of quantum cryptography is found in classical cryptography we shall have to take a step back into the world of classical code making before examining some of the more recent theoretical developments arising from quantum coding. In the next section, therefore, we shall briefly look at classical cryptography, our aim being to show why quantum cryptography is potentially so important. The invention of the first quantum cryptography protocol is, in our opinion, one of the most important advances in quantum processing and we shall, accordingly, spend a little time describing this remarkable development. Having laid the foundations, we shall explore the practical consequences of these ideas and show how the new theoretical approaches have helped us home in on the likely candidates for practical implementation.

If quantum cryptography is to succeeed as a viable method for protecting data on real communication systems, it must be capable of implementation on optical networks. In other words, the focus of its applicability, if it is to be widespread, must shift from *point-to-point* links to distributed communications networks. We have developed several techniques for achieving this aim. In the final section we shall take a brief look at this and other future possibilities for processing data at a quantum level. In particular, recent developments in quantum computing have seriously brought into question the long-term security of certain widely used encryption techniques. If the inherent potentialities of quantum computing are fully utilized, quantum cryptography may well be the only defence against the quantum code breakers of the future!

1.2. *What is the problem with classical codes?*

In short, the answer to this question is 'nothing'. It has been known for many years [10] that it is possible to design an unbreakable code.† In fact, it is remarkably easy to do so. One might be forgiven, therefore, for wondering why we need professional cryptologists at all. In order to answer this question we need to understand a little more about the process of cryptography and cryptanalysis. Cryptography is the art of taking a message, known as the plaintext, and rendering this message unreadable to any unauthorized person. This is usually done by the process of encryption. Encryption works by taking an additional secret, known as the key, and using this to 'scramble' the plaintext, thus converting it into the ciphertext, or cryptogram. The idea is that without the key to unlock the plaintext from the ciphertext the cipher system should be unbreakable, that is it should be impossible to recover the original message from the ciphertext without the key. Cryptanalysis is the art of uncovering the plaintext, and possibly the secret key, from the ciphertext. If we consider the word LASER as our plaintext to be encrypted, then we see that a simple substitution such that each letter of the alphabet moves up one to its neighbour will produce the ciphertext MBTFS. In this case we have used a specific algorithm (move the letter up by a certain amount) together with a key (the number of places to move, in this case one) to produce the scrambled message. With knowledge of the key it is immediately possible to recover the plaintext LASER from the ciphertext MBTFS. Admittedly this is not a very secure cipher system but it illustrates the fact that it

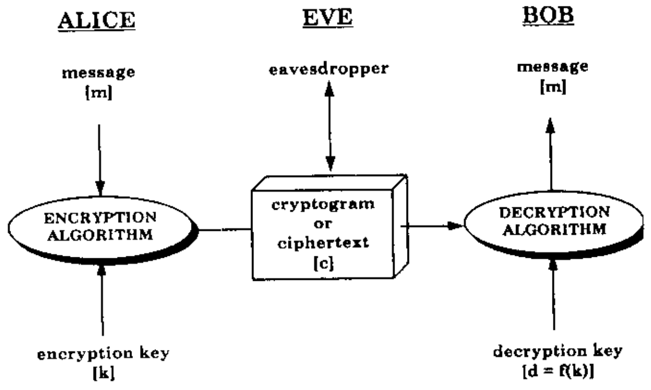


Figure 1. The basic elements of a cipher system. Alice feeds in the message *m* together with the encryption key *k*, to the encryption algorithm which produces a resultant ciphertext *c*. Bob receives the ciphertext and feeds this, together with the decryption key *d*, into the decryption algorithm to recover the message. The decryption key does not have to be the same as the encryption key but, for symmetric cipher systems, it should be easily derivable from it.

†We should not use the word code in this context. A more correct terminology would be cipher system. A message can be coded without any attempt at secrecy, an example being the coding of the roman alphabet into binary, or indeed Morse code. When an attempt to communicate secretly through the use of coding techniques is made, the system used to do this is referred to as a cipher system or cryptosystem and the resulting text is referred to as ciphertext or the cryptogram.

is important to keep knowledge of the key secret. In the above example a cryptanalyst might have to check all possible 26 keys† to recover the message, whereas the plaintext is immedately recoverable with the key.

The elements of a cipher system are depicted in figure 1 where we have adopted the usual terminology of Alice to describe the transmitter, Bob to describe the receiver and Eve to describe the unauthorized eavesdropper who wishes to read the plaintext that Alice is trying to send securely to Bob. Thus Alice encrypts the plaintext message **m** with a specified algorithm and secret key **k** and transmits the resultant cryptogram **c** to Bob who uses the inverse algorithm and some easily computable $\mathbf{d} = \mathbf{f}(\mathbf{k})$ as a decryption key to decrypt the ciphertext back into the plaintext message. An eavesdropper Eve has access to **c** and probably the algorithm used to encrypt, but she is assumed not to have access to **k** or **d**. There are examples of cipher systems in current use where the encryption and decryption algorithms are well known and in the public domain. For these systems the security resides *entirely* in the secrecy of the key. The key and its secrecy are clearly of central importance to the security of the entire cipher system. It is therefore important to understand the precise role of the key.

We have used the term unbreakable in the above discussion and its intuitive meaning is clear. There is, however, a precise definition of this concept, introduced by Shannon [10], which is more commonly called perfect secrecy. A cryptosystem is said to exhibit perfect secrecy if a cryptanalyst Eve gains no extra information about the plaintext message **m** from obtaining the ciphertext **c**. In other words for perfect secrecy we would require the message to be statistically independent from the ciphertext. If $P(\mathbf{m}|\mathbf{c})$ is the probability of obtaining the message **m** from the ciphertext **c**, then Shannon's definition of perfect secrecy implies that

$$P(\mathbf{m}|\mathbf{c}) = P(\mathbf{m}) \tag{1.1}$$

for all **m** and **c** so that Eve's probability of obtaining the message is the same with or without the cryptogram, i.e. the best that Eve can do is simply to guess. Knowing the ciphertext gives Eve no advantage in a perfect secrecy cipher system. Another requirement we would expect from such a system is that any message can give rise to any ciphertext with equal probability. This is encapsulated in the equivalent definition of perfect secrecy, which follows from equation (1.1) by application of Bayes' theorem, and states that

$$P(\mathbf{c}|\mathbf{m}) = P(\mathbf{c}) \tag{1.2}$$

for all **m** and **c** so that Eve's probability of obtaining a particular ciphertext is independent of which message was sent (if this were not the case, Eve would be able to associate a particular kind of ciphertext with a particular class of message and the cipher system would no longer have perfect secrecy). This latter statement of perfect secrecy implies that the total probability of all the keys that transform a given message into **c** is the same as that of all the keys that transform another message into the same ciphertext. If all keys are equally likely, this means that there are a constant number of keys which transform any given message into a given ciphertext.

It is clear that different messages encrypted with the *same* key must yield different ciphertexts; otherwise there would be no way for Bob, given the ciphertext and key, to determine the original message. In other words there must be at least as many ciphertexts as there are messages. Perfect secrecy now implies that the number of possible keys must also be at least as great as the number of possible messages. If this were not so, there would be some messages that would not be encrypted to a particular ciphertext and obtaining that ciphertext would allow a cryptanalyst to discard those messages. Further discussion of theoretical perfect secrecy can be found in [11].

The simplest cipher system to guarantee perfect secrecy is the one-time pad proposed by Vernam [12] in 1926 but not proven to be theoretically secure until Shannon's [10] work. We follow here the discussion given in [13] but we shall concentrate on binary alphabets. Imagine that we wish to send an N-letter plaintext message **m** in perfect secrecy. The one-time pad achieves this by taking a random N-letter key string **k** and adding this (modulo the alphabet size) letter by letter to the message to obtain the ciphertext **c**. The four possible additions (mod 2) in binary are

$$\begin{array}{r} 1\ 0\ 1\ 0 \\ \oplus 1\ 1\ 0\ 0 \\ \hline 0\ 1\ 1\ 0 \end{array}. \tag{1.3}$$

Thus we have a ciphertext, produced according to the rule (1.3) given by

$$\mathbf{c} = \mathbf{m} \oplus \mathbf{k}. \tag{1.4}$$

To decipher this, Bob simply takes his copy of the key and subtracts it (modulo the alphabet size) letter by letter from the ciphertext, giving

$$\mathbf{m} = \mathbf{c} - \mathbf{k}. \tag{1.5}$$

In the case of binary, of course, subtraction (mod 2) is equivalent to addition (mod 2). Eve, we have assumed, knows **c** but not **k**. Suppose that she tries to obtain **m** by guessing the key. She tries some $\mathbf{k}'$ to obtain

$$\mathbf{m}' = \mathbf{c} - \mathbf{k}'. \tag{1.6}$$

Because $\mathbf{k}'$ is simply a random bit string of equal length to the message, $\mathbf{k}'$ could also have been chosen by Alice and Bob as their key so that $\mathbf{m}'$ could be any one of $2^N - 1$

†Of course, although there are 26 possible keys, one of them will shift the ciphertext back on to the message, a possibility that one might wish to avoid!

messages (assuming that $\mathbf{k} \neq \mathbf{k}'$). Eve's problem is not one of finding a plaintext, it is simply that she can find too many and cannot choose between them. Thus she is equally likely to decipher the message 'meet me at 5 o'clock' as 'meet me at 6 o'clock' and without further knowledge she cannot choose between them.† Searching through all the possible keys is of no help; amongst all the possible messages will be the correct version, but how is Eve to distinguish this from the others?

It can be shown from the conditions (1.1) and (1.2) that the one-time pad does indeed yield perfect secrecy [11, 15] provided that the key is a *random bit string as long as the message* and is used only once. This latter condition is intriguing, but it is disastrous to ignore this requirement. Using the same key twice to encipher two different plaintexts under a one-time pad is a cipher system that is easily broken so that both plaintexts *and* the key can be obtained. This is because, if we add two ciphertexts $\mathbf{c}_1$ and $\mathbf{c}_2$ that have been produced from two different messages $\mathbf{m}_1$ and $\mathbf{m}_2$ from the same key $\mathbf{k}$, we find that

$$\begin{aligned}\mathbf{c}_1 \oplus \mathbf{c}_2 &= (\mathbf{m}_1 \oplus \mathbf{k}) \oplus (\mathbf{m}_2 \oplus \mathbf{k}) \\ &= (\mathbf{m}_1 \oplus \mathbf{m}_2) \oplus (\mathbf{k} \oplus \mathbf{k}) = \mathbf{m}_1 \oplus \mathbf{m}_2,\end{aligned} \tag{1.7}$$

where we have used the fact that under addition (mod 2) each element is its own inverse. Knowing the addition of two messages gives the eavesdropper a significant advantage. In fact using the key twice in a one-time pad is equivalent to using one of the plaintexts as a key in a running-key cipher [13] and this cipher system can be readily broken.

The above discussion has emphasized a particular kind of cipher system giving perfect secrecy. It is surprisingly easy to design such a system, the one-time pad being the classic example. However, the major problem with systems of this kind is that the key needs to be as long as the message, and it needs to be kept secret, of course. Alice and Bob need to find some way of exchanging the key $\mathbf{k}$ to keep it secret.‡ It is a classic 'Catch 22' situation; we need to communicate in secret and there exist perfectly good techniques to achieve this *provided* that we can communicate in secret . . . . For some communications of considerable importance and where expense is not an issue, keys for use in a one-time pad are exchanged by courier-based methods. Such key exchanges are slow, expensive and never fully guaranteed. In classical cryptography the largest practical issues of concern are the very real problems of key management, distribution and generation. Using quantum mechanics to provide absolute secrecy is an intriguing prospect.

1.3. *Practical security and quantum cryptography*

People want their messages to be secure. Few of us would wish our private conversations overheard no matter how innocuous. Few of us, however, are willing or able to go to the expense and complication of distributing long keys for use in a one-time pad. Cryptographers, faced with the problem of providing convenient inexpensive security, have devised many solutions. These solutions arise from a realization that, for many purposes a cipher system does not need to be unconditionally unbreakable. It may be, for example, that after a few days it is no longer essential to protect information (an example of this may be the protection of share-sensitive information before company mergers). A cipher system then may only be needed to provide a high level of security for a certain length of time. This length of time should be short compared with the 'cover time' of a cipher system which is an estimate of how long it will take a dedicated eavesdropper using sophisticated equipment to obtain the message (and possibly the key) from the ciphertext. For police vehicles, for example, in rapid-response situations it may only be necessary to employ a cipher system with a cover time of a few minutes ensuring *practical* security with little cost and/or complexity. The simple substitution cipher, discussed above, which was used to encipher the word LASER has an extremely short cover time, the cryptanalyst only having to search through 25 keys to recover the message, an easy task on a modern computer. An attack which examines each possible key is known as an exhaustive key search. Exhaustive key searches are not effective with one-time pads because each key yields a legitimate message. However, suppose a cipher system is designed to use a key of 56 bits in length. An exhaustive key search would have to sample all 2^{56} possible keys; quite an undertaking even on modern computers. Modern cipher systems are thus geared towards providing a high level of security with shorter keys.¶

Some level of secrecy, albeit less than the perfect secrecy theoretically possible, is readily available through well known cipher systems. Perhaps the most famous of these is the Data Encryption Standard (DES) first published in 1975 by the US National Bureau of Standards [11]. In its 'standard' application, DES is seeded with a key of 56 bits in length and uses this to encrypt the input plaintext with a *publicly known algorithm*. For a computer able to check 1 million keys per second an exhaustive key search on a DES-encrypted

†In skipping to an English text, by way of example, we have neglected some subtleties associated with redundancy and coding. The interested reader is referred to [11, 14].

‡For non-interactive messages this, of course, begs the question of why they do not just send their actual message secretly in this way as the key needs to be as long as the message.

¶In some applications a short key is used to seed a random number generator (RNG) for use in a one-time pad. Knowing the short key and the particular RNG will enable the entire random sequence to be reproduced. Thus an eavesdropper knowing these two features can reproduce the entire keystream.

ciphertext would take over 2000 years! A computer able to check 1 million million keys per second would be able to decrypt a DES ciphertext in just under a day! In its standard application DES is clearly not future proofed against the phenomenal advances expected in computational power. Although DES is used in more sophisticated ways than its standard application and indeed cryptanalytic techniques are also a good deal more sophisticated than simply checking all possible keys, it is fair to say that DES has never been broken in any meaningful way (at least not in public!). This is quite a remarkable achievement given its 20 year history and the efforts that have been made to find weaknesses in DES. If for practical security at this level it is sufficient to distribute keys of around 100 bits the key management and distribution problems are much less severe than those faced by the one-time pad. Nevertheless, because algorithms such as DES are in the public domain, any DES encrypted ciphertext remains unreadable to an eavesdropper *only* because the key is kept secret. Once again we are faced with the problem of getting a small random sequence, a key of length 56 bits, say, from Alice to Bob in such a way that it is kept secret. It would be nice if there were an automated communication system that could establish an identical random sequence of bits, for use as a cryptographic key, in two physically separate locations, in such a way that any attempt to listen in on the channel can be detected and effectively dealt with.† This is precisely what a quantum cryptography system does! How this is achieved is arguably one of the most fascinating episodes in quantum processing.

2. A brief history of quantum cryptography

2.1. *The BB84 Protocol: the fundamental quantum properties*

The first complete protocol for exchanging keys in secret using quantum cryptography was published in 1984 [17]. This protocol is now known amongst quantum cryptographers as the BB84 protocol. BB84 is a development of the earlier ideas for using quantum mechanics to protect data [2, 18]. Whilst there have been many important studies (for example [19]) to discover the limits to information flow on communication channels imposed by quantum mechanics, the BB84 protocol and its antecedents [2, 18] represent the first time, to our knowledge, that the quantum peculiarities of nature have been *directly exploited* to give a fundamental advantage in information processing.‡ It is difficult to overemphasize the importance of quantum cryptography for our understanding of quantum information processing (see [21] which is a special issue containing a collection of papers dealing with the whole area of quantum information processing). Together with the recent advances in quantum computing [22, 23], quantum cryptography has been instrumental in changing our approach from one of finding limits imposed by quantum mechanics to that of asking 'what extra features does quantum mechanics give?'.

We have emphasized in the preceding discussion that quantum mechanics brings extra functionality to communication channels, above that implied by a classical description. The two most important differences between classical and quantum descriptions of the world can be summarized by the words complementarity and correlation. Both of these properties can be exploited to give quantum-cryptographically protected communications, but we shall concentrate initially on the former property of complementarity and the essential features of quantum mechanics necessary to understand the workings of the BB84 protocol. In simple terms the essence of complementarity is that measurement of a quantum system disturbs it. An experiment can be designed to probe either the particle-like or the wave-like properties of a quantum system, for example, *but not both.* The particle and wave aspects are said to be complementary attributes of a quantum system. The classic example of this is Young s double-slit experiment for single 'particles'. If we try to determine through which slit a particle went, thus probing the particle-like nature of the system, we lose any interference pattern. If we choose to view the interference pattern, thus probing the wave-like nature of the system, we cannot determine through which slit the particle went. Complementarity is one of the central mysteries of quantum mechanics. Richard Feynman wrote in his celebrated *Lectures on Physics* [24] that this phenomenon or property is one which '. . . is impossible, *absolutely* impossible, to explain in any classical way, and which has in it the heart of quantum mechanics'. This complementarity finds its rigorous expression in the incompatibility of quantum observables; by which we mean that, if $\hat{A}$ and $\hat{B}$ are the quantum operators representing two physical observables of a quantum system, then these observables are said to be incompatible if

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} \neq 0, \qquad (2.1)$$

that is they do not commute.

†It will not have escaped some readers' attention that we have completely neglected public-key or asymmetric cipher systems in the above discussion. Public-key cryptography [16] was developed in response to the key distribution problems faced by conventional cryptosystems. It is our belief that quantum key distribution and, in particular, recent results in quantum computing, may force a re-examination of the assumptions upon which public-key cryptography was developed. We shall return to this point in the concluding sections.

‡Of course, squeezed states of light (see [20] which is a special issue containing a collection of papers on squeezing and in particular the review article in that issue by Loudon and Knight) can be used to give improvements in signal-to-noise ratio in communication systems beyond those possible with classical sources. However, quantum cryptography has shown that radically different *functionality* can be achieved with quantum communication channels.

The properties associated with incompatible observables will, to a greater or lesser extent, be complementary and measurement of one will disturb the other. One of the consequences of equation (2.1) is the Heisenberg uncertainty relation which connects the variances of two operators to the commutator (2.1) by the following inequality:

$$\langle(\Delta\hat{A})^2\rangle\langle(\Delta\hat{B})^2\rangle \geqslant \tfrac{1}{4}|\langle[\hat{A},\hat{B}]\rangle|^2. \tag{2.2}$$

Precise measurement of one property will result in a 'fuzziness' associated with any complementary property. This is often phrased as an impossibility to know, with arbitrary accuracy, both of the incompatible properties represented by $\hat{A}$ and $\hat{B}$. In Young's two-slit experiment with electrons, for example, we could try to determine which slit the electron went through by using a photon to 'see' the electron. However, interaction of the electron with the photon imparts a momentum kick to the electron sufficient to destroy the interference pattern. If we try to use photons of a longer wavelength, thereby reducing the momentum kick imparted to the electron, we find that the interference pattern is restored when the wavelength is greater than the slit separation. However, it is then no longer possible to resolve the slits and it is therefore no longer possible to ascribe a unique trajectory to the electron. It is possible to use the existence or otherwise of the interference pattern to determine whether or not an attempt has been made to measure the trajectory of the electron. Turning the experiment on its head in this way and asking whether or not there has been an attempt to tamper with the electron (that is to measure its trajectory), we can see the beginnings of an idea of how quantum mechanics may be used to protect information. Let us pursue this line of thought further.

We begin by following Sakurai [25] rather closely and consider a sequence of selective measurements or quantum state filters. A quantum state filter is designed to allow the passage of a particular quantum state and no other. Suppose that the state $|\alpha_j\rangle$ from the eigenbasis $\hat{A}|\alpha_j\rangle = \alpha_j|\alpha_j\rangle$ is incident on a $\hat{B}$ filter designed to allow the state $|\beta_k\rangle$ from the eigenbasis $\hat{B}|\beta_k\rangle = \beta_k|\beta_k\rangle$ to pass. This situation is sketched in figure 2. The probability that the state $|\beta_k\rangle$ is obtained from the filter given an incident $|\alpha_j\rangle$ is determined from the usual quantum expansion coefficients to be $|\langle\alpha_j|\beta_k\rangle|^2$. In other words we have

$$|\alpha_j\rangle = \sum_k |\beta_k\rangle\langle\beta_k|\alpha_j\rangle \tag{2.3}$$

and when making a measurement of the property represented by $\hat{B}$ the quantum rules tell us that the probability of obtaining the eigenvalue β_k is the square modulus of the overlap $\langle\beta_k|\alpha_j\rangle$. After the measurement the state is projected into the corresponding eigenstate of $\hat{B}$. However, we can equally well envisage the alternative expansion of $|\alpha_j\rangle$ in the eigenbasis of another operator $\hat{E}$ so that

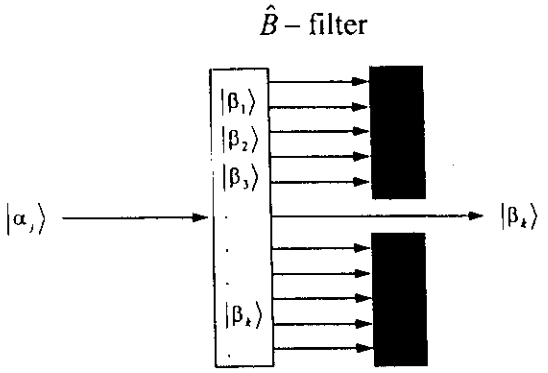


Figure 2. A schematic illustration of a quantum state filter designed to allow only the state $|\beta_k\rangle$ to pass. This is equivalent to performing a selective measurement in which only a particular result is acceptable and all others are discarded.

$$|\alpha_j\rangle = \sum_m |\varepsilon_m\rangle\langle\varepsilon_m|\alpha_j\rangle. \tag{2.4}$$

The probability of obtaining $|\beta_k\rangle$ given an incident $|\alpha_j\rangle$ can now be written as

$$\begin{aligned}|\langle\alpha_j|\beta_k\rangle|^2 &= \left|\sum_m \langle\alpha_j|\varepsilon_m\rangle\langle\varepsilon_m|\beta_k\rangle\right|^2 \\ &= \sum_m\sum_{m'} \langle\alpha_j|\varepsilon_m\rangle\langle\varepsilon_m|\beta_k\rangle\langle\beta_k|\varepsilon_{m'}\rangle\langle\varepsilon_{m'}|\alpha_j\rangle.\end{aligned} \tag{2.5}$$

We can think of $|\alpha_j\rangle$ as being 'made up' of the states $|\varepsilon_m\rangle$ and the eventual probability $|\langle\alpha_j|\beta_k\rangle|^2$ can be viewed as resulting from an interference of all the possible paths of the kind $|\alpha_j\rangle \rightarrow |\varepsilon_m\rangle \rightarrow |\beta_k\rangle$. The interference pattern in a two-slit experiment is caused by the quantum interference between the two possible paths distinguished by the two slits.

Now let us consider the arrangement in figure 3 where an $\hat{E}$ filter has actually been inserted before the $\hat{B}$ filter. If the $\hat{E}$ filter is set to admit the state $|\varepsilon_m\rangle$, then the probability P of obtaining $|\beta_k\rangle$ given an input $|\alpha_j\rangle$ is now given by

$$P = |\langle\alpha_j|\varepsilon_m\rangle|^2|\langle\varepsilon_m|\beta_k\rangle|^2. \tag{2.6}$$

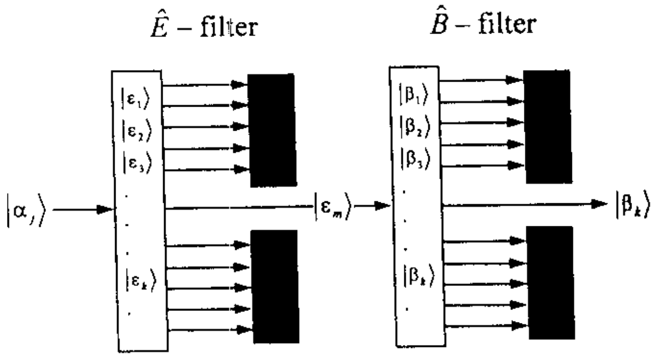


Figure 3. A sequence of two quantum state filters designed to allow only the state $|\beta_k\rangle$ to pass.

To obtain the total probability we must sum over all possible filter settings so that

$$\begin{aligned} P &= \sum_m |\langle \alpha_j | \varepsilon_m \rangle|^2 |\langle \varepsilon_m | \beta_k \rangle|^2 \\ &= \sum_m \langle \alpha_j | \varepsilon_m \rangle \langle \varepsilon_m | \alpha_j \rangle \langle \beta_k | \varepsilon_m \rangle \langle \varepsilon_m | \beta_k \rangle, \end{aligned} \tag{2.7}$$

which is clearly, in general, *not equal* to equation (2.5). By examining the statistics from the $\hat{B}$ filter it is possible to determine whether or not the $\hat{E}$ filter has been applied. The interference terms have been suppressed in equation (2.7) and we can write equation (2.5) as

$$|\langle \alpha_j | \beta_k \rangle|^2 = P + \sum_{\substack{m \\ (m \neq m')}} \sum_{m'} \langle \alpha_j | \varepsilon_m \rangle \langle \varepsilon_m | \beta_k \rangle \langle \beta_k | \varepsilon_{m'} \rangle \langle \varepsilon_{m'} | \alpha_j \rangle, \tag{2.8}$$

the second term containing the interference contribution from the possible $|\{\varepsilon_m\}\rangle$ paths. In the two-slit experiment the $\hat{E}$ filter is equivalent to determining the precise trajectory of the particle and equation (2.7) is a mathematical expression of the consequent destruction of interference.

Under what conditions will it *not* be possible to tell whether a measurement has been made on the particle before it gets to the $\hat{B}$ filter? This occurs when equations (2.5) and (2.7) are identical and the condition for this is given by

$$\langle \alpha_j | \varepsilon_m \rangle \langle \varepsilon_m | \beta_k \rangle \langle \beta_k | \varepsilon_{m'} \rangle \langle \varepsilon_{m'} | \alpha_j \rangle = \delta_{mm'}. \tag{2.9}$$

This condition can only be satisfied if $|\varepsilon_m\rangle$ is a simultaneous eigenstate of both $\hat{E}$ and $\hat{A}$ (and/or $\hat{B}$). For this to be the case $\hat{E}$ and $\hat{A}$ (and/or $\hat{B}$) must be *compatible* observables; in other words we must have

$$[\hat{A}, \hat{E}] = 0 \text{ and/or } [\hat{B}, \hat{E}] = 0. \tag{2.10}$$

The action of the $\hat{E}$ filter can only be detected if $\hat{E}$ represents a complementary property to *both* of the properties represented by $\hat{A}$ and $\hat{B}$. This is also true if $\hat{A}$ and $\hat{B}$ are themselves compatible observables, that is, they commute, in which case they have a simultaneous eigenbasis. It is the ingenious exploitation of the properties of complementary observables that enables the BB84 protocol, and indeed some of the other protocols that have been invented, to offer guaranteed secure key distribution. The security of the data is guaranteed by the fundamental properties of quantum observables. It is impossible to know with arbitrary accuracy the properties of two incompatible observables. This fundamental result is encapsulated in the Heisenberg uncertainty relation between two complementary observables. The BB84 protocol exploits this by choosing a random coding scheme between a pair of such observables. It could be said, therefore, that quantum key distribution can only be 'broken' by violation of the Heisenberg uncertainty principle! Such a possibility is disallowed by quantum mechanics; if complementarity were to fail, then so would quantum mechanics. This property of complementarity is central to the security of a quantum key distribution scheme and an appreciation of this allows some rather general theorems about quantum key distribution channels to be derived [26].

Table 1. Notation and coding for the circular and linear polarization states of single photons

State	Coding
Right circularly polarized $\lvert R\rangle_{\text{circ}}$	1
Left circularly polarized $\lvert L\rangle_{\text{circ}}$	0
Vertically polarized $\lvert 0\rangle_{\text{linear}}$	1
Horizontally polarized $\lvert \pi/2\rangle_{\text{linear}}$	0

2.2. *The BB84 protocol: a brief introduction*

The discussion above has highlighted some of the general features of quantum mechanics that are exploited in quantum cryptography. We shall concentrate here on the specific implementation of quantum key distribution developed by Bennett and Brassard now known as the BB84 protocol [17]. The quantum systems that can be used to implement the BB84 protocol are two-state systems, that is they are spanned by a Hilbert space of dimension 2. Examples of such quantum systems are spin-$\frac{1}{2}$ particles, two-level atoms and the polarization states of single photons. Each of these systems can be described by the same mathematics, that of Pauli spin algebra, even though they are quite distinct physical systems. In the case of photon polarization, for example, a particular photon prepared in a state of circular polarization can be right circularly polarized or left circularly polarized, the left and right circularly polarized states forming the basis spanning the two-dimensional Hilbert space. Equally, the two linear polarization states, 'vertical' and 'horizontal', form a basis spanning the space. All the photon's polarization properties can be understood in terms of either of these two polarization bases, or linear combinations of the states therein. The polarization state space is formally equivalent to the space spanned by the two spin states of a spin-$\frac{1}{2}$ particle. Thus, for example, we can make a formal identification between the 'up' and 'down' spin states in the z direction, say, and the vertical and horizontal polarization states of a linearly polarized photon. In what follows we shall use a polarization basis to describe the BB84 protocol, although the results are true for any two-dimensional quantum system. The notation for the polarization states is summarized in table 1.

Before we describe the protocol in some detail we shall take a look at the various possible measurements of the polarization states of a single photon and their interpretation. Suppose that you were given a photon and told it was prepared in one of the four polarization states $|L\rangle_{\text{circ}}$, $|R\rangle_{\text{circ}}$, $|0\rangle_{\text{linear}}$ and $|\pi/2\rangle_{\text{linear}}$ but not which one of those states and asked to identify which particular state; which measurement would you choose? In fact there is no single measurement, or sequence of measurements, that will enable you to determine unambiguously the polarization state of the photon. This occurs because the operators representing measurements of linear polarization and circular polarization in the given directions are incompatible. Suppose that in fact you had been given a photon prepared in the state $|R\rangle_{\text{circ}}$. If you decided to measure a circular polarization, all well and good, you would identify the state with 100% accuracy (assuming perfect measuring apparatus). However, if you had chosen to measure a linear polarization along the given direction, you would obtain the result $|0\rangle_{\text{linear}}$ with 50% probability and the result $|\pi/2\rangle_{\text{linear}}$ with 50% probability. This is because the circularly polarized state $|R\rangle_{\text{circ}}$ can be written as an expansion in the linear polarization basis as

$$|R\rangle_{\text{circ}} = \frac{1}{2^{1/2}}(|0\rangle_{\text{linear}} + \mathrm{i}|\pi/2\rangle_{\text{linear}}). \qquad (2.11)$$

However, the situation is worse than it appears at first sight; not only do you obtain a probabilistic result with the 'wrong' measurement but also you do not know that you have obtained such a result! All that can be said after a particular measurement is that the photon is now in the state measured. You might be tempted then to copy the photon so that you could measure different properties on the identical copies. However, in order to copy the photon you would need to know its state and copying a photon precisely would necessarily entail making a measurement of its state. If you could do that you would not need to copy it in the first place! This 'no cloning' property of single quanta is a consequence of the general structure† of quantum mechanics [27] and is a rather important result for quantum cryptography.

You could be interested in a slightly different question; what bit does the photon represent? In other words can we determine whether it is a 1 or a 0 according to the coding scheme given in table 1. In this case, measurement in the correct basis yields the bit with 100% accuracy. Measurement in the other basis will yield a random result; so overall you are 75% likely to get the correct result on a single measurement (provided that of course you do not choose one measurement basis more often than the other). Of course measurement of circular polarization and linear vertical or horizontal polarization as we have described does not cover all the possible measurements that you might want to make. For example, you might want to make a measurement of linear polarization aligned at some other angle θ where the result of the measurement would be one of the two linear polarization states $|\theta\rangle_{\text{linear}}$ or $|\theta + \pi/2\rangle_{\text{linear}}$ with probabilities determined by the choice of angle. Measurements of this kind are discussed in [28]. Another strategy might be for you to interact the photon with another system and to make a measurement on that system. Because of the wide variety of possible measurement strategies we shall concentrate only on those of most importance. It is important to recognize, however, that whatever strategy is chosen it is impossible, *in principle*, to determine accurately the state of the photon when you are told only that it has been coded in one of two incompatible bases, but not which one.

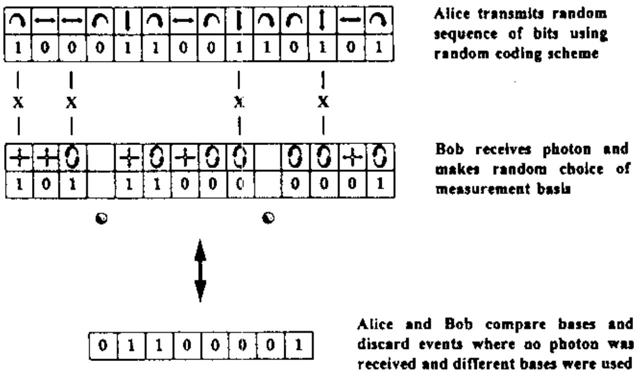
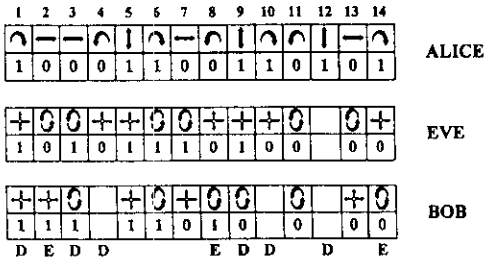

1 0 0 0 1 1 0 0 1 1 0 1 0 1
Alice transmits random sequence of bits using random coding scheme
X X X X
1 0 1 1 1 0 0 0 0 0 0 1
Bob receives photon and makes random choice of measurement basis
0 1 1 0 0 0 0 1
Alice and Bob compare bases and discard events where no photon was received and different bases were used

Figure 4. An example of a quantum transmission between Alice and Bob. There are 14 time slots in the transmission. In four of these slots Bob measures the wrong basis and these are indicated by X. In two of these slots, indicated by a ©, Bob does not register a count. In the other eight instances Bob measures the correct basis so that Alice and Bob eventually establish an 8 bit random binary sequence as their key.

Having briefly examined some of the implications of incompatible observables we shall now describe in some detail the BB84 protocol. The essence of the protocol is contained in figures 4 and 5. Alice begins by generating a random bit sequence. This is used to select a bit value, either 1 or 0, and the polarization basis of the photon in which that bit is to be encoded. Having generated the random sequence, and having thereby decided on the coding, Alice generates



Bit positions 1,3,4,5,10 and 12 are discarded
Bit positions 2,8 and 14 lead to an error caused by Eve
Bit position 12 is an extra 'null' event caused by Eve

Figure 5. The same quantum transmission shown in figure 4 but with the presence of an eavesdropper. The 8 bit random binary key sequence of figure 4 has now been changed by the intervention of the eavesdropper.

†The no-cloning theorem disallows the possibility of copying an arbitrary quantum state. This result is a consequence of the linear superposition principle of quantum mechanics.

the photons in the required state and sends them on to Bob over an optical link that is not necessarily private. We assume, for the purposes of the present discussion, that the photons are generated in a regular sequence so that only one photon is present in any given time slot. We shall return to the question of timing when we describe the current experimental implementations. Bob receives this regular sequence of photons and for each time slot chooses, randomly and independently of Alice, a measurement basis in which to determine the photon's polarization state. This procedure is shown in figure 4 where an example 14 bit sequence is shown with the coding chosen by Alice. Bob's measurements are shown directly below the bits chosen by Alice. We can see that one of three things can happen: Bob does not receive the photon, Bob makes an incorrect choice of measurement basis, or Bob measures in the correct basis. Alice and Bob now engage in a public discussion and exchange basis information, that is they disclose the coding and measurement bases chosen, *but they do not disclose the actual bits.* Those instances where Alice and Bob chose different bases are discarded as no correlation between sent and received data is expected. Bob and Alice also discard those time slots where no photon was received by Bob. Alice and Bob keep the remaining time slots and should therefore now share an identical sequence of random bits. It is the fact that any eventual key is only established from those bits *actually received* by Bob that makes a quantum key distribution scheme robust to loss. Loss does not compromise the security of the system but merely reduces the data rate of the key exchange. Because Alice and Bob are making random and independent choices of coding and measurement basis respectively, they would expect, as a result of this public discussion, to have thrown away around half of the time slots where Bob registered a result. The random choice of bases is important for the security because it means that any eavesdropper, and indeed Bob himself, must guess the correct basis in order to receive a key bit.

What happens when Eve tries to listen in? Because both Alice and Bob are using a random coding and measurement scheme respectively, Eve cannot know before the transmission which bits are going to be useful. Her only option is to somehow measure the polarization state of the photons sent by Alice and to send them on to Bob. She cannot simply be a passive intruder; the final key is only established from bits actually received by Bob. Furthermore, she can only guess as to the coding basis for any particular photon. If she decides to read the bit encoded on any particular photon, she must choose a measurement basis to do so. It is possible, and indeed quite likely, that the basis she chooses will not be the correct basis. Unless Eve has specifically chosen a basis not used by Alice or Bob (for reasons we shall come to), there is no way for her to know whether her measurement has been successful in reading the correct bit and sending on the correct state to Bob. The random coding and measurement scheme of Alice and Bob is designed to force Eve to make errors. If we consider a specific instance where both Alice and Bob have chosen the same basis and Eve has guessed incorrectly and chosen the complementary basis, then there is a 50% likelihood that Eve reads the wrong bit. For example, if we suppose that Alice has transmitted a 1 encoded on the photon polarization state $|0\rangle_{\text{linear}}$ and that Eve has measured in a circular polarization basis and obtained the result $|L\rangle_{\text{circ}}$, then Eve will interpret this as a 0. Furthermore, only those bits that reach Bob will form part of any eventual key so that Eve must send something on to Bob if her measurement is to be useful to her. At this point Eve does not know which basis was used by Alice and does not know which measurement basis is to be chosen by Bob. What should Eve do? Clearly, if Eve wants the information she must do something. Let us suppose that she sends on the photon in the state she measured (what reason has she, at this point, for choosing any other option?). The photon that Bob receives is therefore in a state of circular polarization and Bob's measurement in a linear basis has only a 50% chance of registering the state $|0\rangle_{\text{linear}}$ and reading the correct bit. We shall suppose the worst case for Eve: Bob actually measures the state $|\pi/2\rangle_{\text{linear}}$ and thus obtains the bit 0. In the public discussion phase, Alice and Bob will keep the result of this time slot as they both used the same basis. However, if they decide to disclose the actual transmitted and received bit for this time slot, they will note the discrepancy where none was expected. The presence of an intruder can then be inferred.

The protocol that Alice and Bob adopt is specifically designed to force Eve into a situation whereby for a fraction of the transmitted bits she cannot avoid introducing errors if she tries to recover the data. If Eve is herself randomly choosing between the two complementary polarizations and retransmitting the photon in the state measured, then she has a 25% chance, per photon, of inducing an error in Alice and Bob's potential key data. That is, 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 the data if Eve has tried this eavesdropping strategy is $(\frac{3}{4})^N$. This attack by Eve is shown schematically in figure 6. In order to test for the presence of Eve, Alice and Bob have a further public discussion where a subset of the remaining bits are randomly chosen and publicly compared. If Alice and Bob select M test bits, say, from their original transmission of N bits, the probability that Eve escapes detection for $M = 100$ is about 3×10^{-13}. After public disclosure of these test bits they are, of course, discarded. From this publicly compared sample, Alice and Bob can reliably estimate an error rate for their data and infer the presence of a malicious influence, Eve, on their communication. This procedure is illustrated in figure 5 where the transmission example shown in figure 4 is repeated with an example active interception by Eve. In this figure, Eve is assumed to have tried to intercept all of the

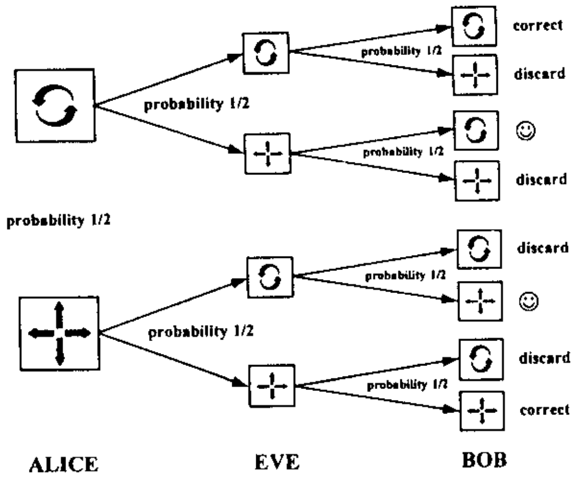


Figure 6. Probability tree for the polarization-encoded BB84 protocol with the effect of an eavesdropper measuring in the transmission bases included. There are eight possible outcomes for Bob. Of these, a quarter lead to reception of the correct bit and these are labelled as such. About half of the possible outcomes are discarded during the public discussion phase. We see that on the remaining pathways, indicated by ☺, Eve will cause an error with a 50% probability. The probability that Eve does not cause an error is therefore three quarters.

transmissions and to have randomly chosen between the linear and circular measurement bases, retransmitting her measured state faithfully. In time slot 1, Eve guessed incorrectly, but so did Bob, and this bit is discarded at the public discussion phase. Time slot 2, however, is an example of a successful tranmission by Alice in that both she and Bob chose the same basis. Eve guessed incorrectly in this instance and has given rise to a discrepancy between Alice and Bob's bit strings. Time slot 7 is a similar instance to that of time slot 2, except that Eve's retransmission of the incorrect state has not given rise to an error. Time slot 10 is another example of how Eve can cause a discrepancy. Here, she tries to measure the photon but receives a null result. If Eve is not careful to compensate for these instances, Alice and Bob can infer her presence from an increase in null results. At the end of a public comparison of bases and rejection of incompatible data, Alice is left with a subset of her transmitted bit string given by 01100001. Bob's bit string, which in the absence of Eve should be identical to this, is 11101000. If Alice and Bob now randomly choose bit positions 1, 3 and 8 to compare publicly, they will note two discrepancies and can infer the presence of Eve. Of course Alice and Bob will wish to test many more bits than this to be certain, with negligibly small probability, that their communication has not been intercepted. If they find after public comparison of the randomly chosen sample that there is no detectable presence of an eavesdropper, they can discard these test bits and use their remaining, undisclosed bits as a secret key.

2.3. *Reconciliation and privacy amplification*

In an ideal world the protocol we have described would detect the presence of an eavesdropper if just a single error was found in the test sample. However, we have to make do with imperfect detectors and noisy systems which can give rise to spurious results even in the absence of an eavesdropper. The experimental systems we shall describe in section 3 have an intrinsic bit-error rate of a few per cent. In order to give a guaranteed level of security, Alice and Bob must assume that *all* the errors in their data are due to an eavesdropper. There is, in principle, no way to distinguish between an error caused by an active eavesdropper and a noise-induced error. Alice and Bob, of course, need to share the *same* key. It is clear therefore that in any practical system environmental influences must be accommodated without compromising the security. In other words, Alice and Bob's bit strings must be reconciled by a suitable error correction procedure. Once this public error correction procedure has been performed Alice and Bob will share an identical sequence of bits. Even if Alice and Bob believe their errors to have arisen purely from noise, this cannot be proven absolutely and they must therefore assume that their reconciled bit string is only partially secret. Is it possible to distil a smaller shared secret key from a larger key that is only partially secret? The answer to this question is that it is indeed possible to distil a smaller key with a provable level of secrecy by a procedure known as privacy amplification [1, 29].

The full protocol, including reconciliation and privacy amplification, is shown in figure 7. Alice and Bob perform their raw transmission and establish a sequence of time slots where a photon was received in the correct basis. In an ideal world, and in the absence of eavesdropping, Alice and Bob should now share an *identical* random sequence of bits. We shall call these bit strings the 'raw' keys. With currently available technology, Alice and Bob's versions of the raw key will almost certainly differ. Alice and Bob select a random sample from this sequence and publicly compare the recorded bits. This gives them a good estimate of the error rate on their remaining data. These test bits are then discarded. If their measured error rate based on this sample is above a certain level Q, then privacy amplification and reconciliation cannot be securely performed and the transmission is terminated. This threshold determines the error rate above which an eavesdropper could have enough information about the bit string to render privacy amplification ineffective. Eve gathers this information by making measurements on the single-photon transmission and by listening in on any public discussion. These measurements have to be consistent with the laws of quantum mechanics so that Q gives a limit based on theoretically possible measurements. In practice it is technically infeasible, at present, for Eve to perform the entire set of strategies consistent with quantum mechanics. However, in order to

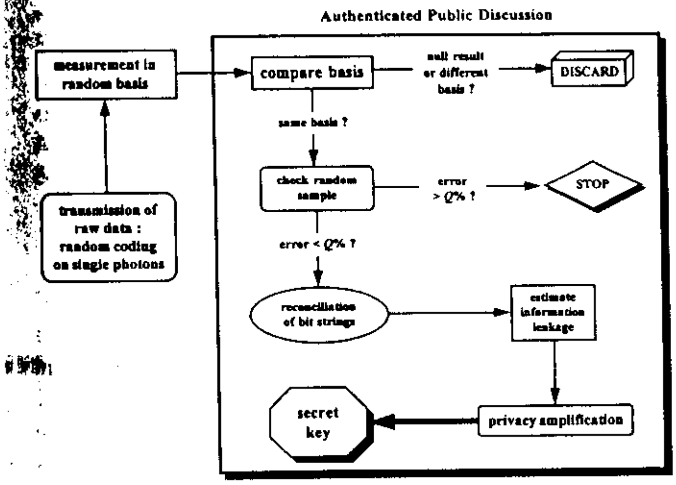

Authenticated Public Discussion
measurement in random basis
transmission of raw data : random coding on single photons
compare basis
null result or different basis ?
DISCARD
same basis ?
check random sample
error > Q% ?
STOP
error < Q% ?
reconciliation of bit strings
estimate information leakage
privacy amplification
secret key

Figure 7. Schematic diagram of the elements of a full implementation of the BB84 protocol. After the quantum transmission an authenticated public discussion is entered into by Alice and Bob. After discarding null results and results arising from different basis choices the level of error on their remaining data is determined empirically by analysing a randomly selected sample of these data and discarding the sample after analysis. If the error is less than a certain amount, the remaining errors in Bob's key data are corrected. Alice and Bob now have identical copies of a random binary sequence that is only partially secret. The final procedure, privacy amplification, distils a smaller sequence, or key, from the error-corrected sequence in such a way that the smaller key is secret to an extremely high confidence level.

give a guaranteed level of security we must suppose that Eve is able to make such measurements. A threshold value of around 10% is our current best estimate of the error rate below which we know our system can be made secure against this powerful Eve [30]. If the measured error rate is below this threshold, then reconciliation and privacy amplification can proceed.

After establishing a raw key and an error rate, Alice and Bob now enter the reconciliation phase of the protocol. After this reconciliation protocol, Alice and Bob should be left with an identical random bit sequence which we shall call the 'reconciled' key. We describe here an adequate but not optimal procedure for locating and correcting the errors in the versions of the raw key. The details are taken from [1]. In this procedure the raw key is shuffled by a publicly agreed random permutation of the bit positions. The purpose of this step is simply to randomize the location of any errors that may have occurred in bursts. The string is then partitioned into blocks of size m such that any block is unlikely to contain more than one error. For each block Alice and Bob publicly compare the parity† and, if this parity check fails, a bisective search is undertaken to locate the error. Each time that a parity bit is disclosed, Alice and Bob discard the last bit of each tested block. In a bisective search, Alice and Bob split their offending block into two parts and publicly compare the parities. The sub-block containing the error will be indicated by this procedure and a further bisective search can be performed to home in on the incorrect bit. Of course this procedure will only locate an odd number of errors, and blocks with matching parity are provisionally accepted as correct. The entire procedure, beginning with random permutation of the bit positions, is performed as many times as is necessary with increasing block sizes until it is estimated that at most only a few errors remain in the entire data set. At this point it becomes very inefficient to continue with a bisective search and a different check procedure is followed in which the parities of a randomly chosen subset of Alice and Bob's entire bit strings are compared. If a disagreement is found, Alice and Bob adopt the bisective search procedure to locate and remove the error. At some point, repetition of this procedure will remove all the errors. After sufficiently many consecutive agreements, Alice and Bob can assume, to a very high level of confidence, that their remaining bit strings are error free. By discarding an extra bit each time that a parity disclosure occurs, Alice and Bob do not leak any extra information to Eve but merely reduce the size of their bit string. The fraction of bits that Eve knows of the reconciled key, because of her eavesdropping, is therefore higher than the fraction that she knew of the raw key.

At this point, Alice and Bob have a reconciled key that is only partially secret. However, from their estimate of the error rate on the raw transmission they can now, in principle, calculate the maximum amount of information that Eve could have obtained consistent with that error rate and the laws of quantum mechanics. Knowing this value, or at least an upper bound, they can enter into the next phase of their public discussion known as privacy amplification. Privacy amplification is a technique whereby a smaller secret bit string can be distilled from a larger only partially secret bit string [29]. It is important to note that, even were we to have access to perfect detectors and communication channels, we would still need privacy amplification to overcome a serious attack by Eve. Of course, any attack by Eve that causes a greater error rate than Q will result in the termination of the key distribution.

Our task now is to find a procedure that will achieve privacy amplification. Surprisingly, perhaps, this turns out to be remarkably simple (*proving* that it achieves security is, of course, non-trivial!). The procedure that we shall discuss here is that of Bennett *et al.* [29] and was used in their original experiments. It is not optimal but has the virtue of being simple and efficient in implementation. Improvements in the procedure have been invented [31]. Suppose that Alice and Bob have a reconciled key of n bits in length and they estimate that Eve can know no more than k bits of this string.

†The parity of a bit string is calculated by forming the sum (modulo 2) of all the bits. If there are an even number of ones, the parity is 0. If there are an odd number, the parity is 1.

In order to reduce Eve's information, Alice and Bob continue to compute $n-k-s$ additional publicly chosen random subset parities in very much the same way as in the final stage of the reconciliation protocol. The parameter s is an arbitrary security parameter that can be adjusted as required. However, instead of revealing the parities of these subsets as was done in the reconciliation stage, Alice and Bob keep these values secret. These undisclosed bits form their final secret key. It can be shown [29] that this procedure reduces Eve's expected information about the final secret key to less than $2^{-s}/\ln 2$ bits.

There is still one piece of the jigsaw missing. How does Alice know that she is talking to Bob and vice versa? In classical cryptography this problem is known as authentication. How do two parties authenticate their communication? By splitting the channel into two and by impersonating Alice to Bob and Bob to Alice, Eve can overcome the quantum key distribution if the public channel is not authenticated. Fortunately for Alice and Bob there exist provably secure authentication techniques for classical channels, provided that the legitimate parties wishing to communicate share some initial secret [32]. In order to overcome this attack by Eve, therefore, Alice and Bob need to have a shared secret to seed the process. They use this initial shared secret to authenticate their public discussion so that Eve is prevented from any active tampering on the public channel. Once a significant amount of secret data is distilled from the quantum key distribution process a portion of these data can be used for authenticating subsequent transmissions.

The last piece is now in place. Authentication is the final tool allowing Alice and Bob to update their keys continually using the full quantum key distribution protocol shown in figure 7. The security of the transmission rests on the Heisenberg uncertainty principle. The level of security of the subsequent classical data-processing techniques has been mathematically established. This beautiful and powerful technique known as quantum cryptography exploits the laws of quantum mechanics in a novel and unexpected way to provide a functionality that cannot be reproduced by classical methods. This technique, together with the emergence of quantum computing, has radically shifted our perspective of quantum data processing. Clever theory and ingenious application are not, however, sufficient to convince everybody! In 1989, quantum cryptography entered a new phase when a collaboration between IBM and the University of Montreal announced that quantum key distribution had been achieved in the laboratory [1]. The few bits per second key rates achieved and the 30 cm distance of transmission in this experiment certainly do not sound very impressive, but to focus on these figures is to miss the point. Quantum key distribution had become a reality and this astonishing concept had grown from pure theoretical invention to practical demonstrator in the space of a few short years. How was it done?

2.4. *The first experimental realization*

The first experimental prototype [1], shown schematically in figure 8, used very faint flashes of light from a green-light-emitting diode to transmit the random sequence of key bits over a free-space link of approximately 30 cm in length. A computer containing software representations of Alice, Bob and Eve was used to control the transmission. Alice's light source produced a beam of incoherent pulses of 5 μs duration at a repetition rate of a few kilohertz. This beam was collimated and passed through a spectral filter and a polarizer. The mean intensity of the beam was very low with an average of about 0·1 photons per pulse. That is, on average only 1 in 10 of the clocked pulses contained a photon. In this way Alice's source approximated a single-photon source and the probability that there is more than one photon per pulse was about 0·005 so that only about 1 in 20 of the pulses containing any photons contained 2 or more. By randomly switching the voltage drive to her Pockel's cell for each pulse, 'Alice' could randomly encode her chosen bit in either a circular or linear polarization basis. Bob's receiving apparatus also consisted of another randomly and independently switched Pockel's cell followed by a calcite polarizer oriented so as to split the beam into horizontally and vertically polarized beams. These beams were directed onto a pair of photomultipliers which had sufficient sensitivity to detect single photons. Bob's choice of basis, linear or circular, was therefore determined by the selected Pockel's cell voltage and the actual bit (1 or 0) by the destination detector.

As anticipated, and as found in practice [1], experimental factors in the real system significantly change the quantum transmission protocol from the ideal case previously discussed. There are several reasons for this. Firstly, Alice does

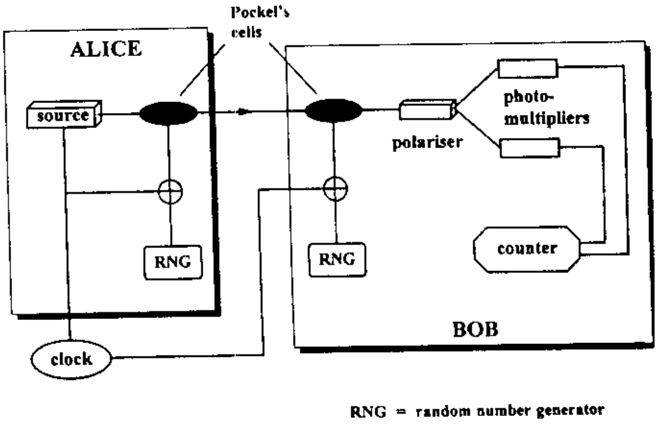


Figure 8. Schematic illustration of the first quantum cryptography demonstrator. Alice's Pockel's cell, driven by a randomly switched voltage, generated a sequence of photons with random coding. Bob's Pockel's cell, driven by an independent randomly switched voltage, selects a measurement basis. Note that Alice and Bob share the same clock sequence but do not share the same random number generator.

not use a single photon source so that there is a chance for Eve to tap off a photon from a multiphoton pulse and make measurements on it whilst remaining undetected. It is for this reason that Alice's source must be operated to produce an extremely low-intensity output that approximates, as closely as can be made practicable, a single-photon source so that the probability of finding more than one photon in any given pulse is very small. Secondly, the detectors used had a relatively low quantum efficiency of around 9%. This means that Bob fails to register the arrival of most of Alice's photons. Any additional loss in the transmission channel itself will reduce further the number of photons measured by Bob. This is, as we have discussed, not a problem in itself because the key is only established from those bits actually measured by Bob so that the security of the channel is not compromised by loss. However, any single-photon measurement system inevitably suffers from noise, i.e. a count is occasionally registered even when no photon is incident on the detectors. They will also occasionally measure the polarization state of an incoming photon incorrectly, owing to misalignment in the optics, for example. This noise occurs randomly and leads to an error rate which, if sufficiently large, can mask the errors caused by an eavesdropper. To alleviate the first problem of 'dark counts', Bob turns his detectors on only in the short time interval during each clock period when he knows a photon may arrive. This is a standard technique for dark count reduction in photon-counting experiments and leads to the requirement that Alice's pulse duration be significantly shorter than the clock period. In order for such a dark count discrimination technique to be effective the number of dark counts still remaining must now only be a fraction of the total received bit rate. This condition places limits on the intensity of the source, the efficiency of the photodetectors and the loss in the transmission channel. The IBM–Montreal team were able to overcome these difficulties and perform a key transmission experiment of about 10 min duration that yielded a key of 105 bits in length such that Eve's expected information about the key was estimated [1] to be about 6×10^{-171} bits!

This is a staggeringly small amount of information indicating an extremely secure key transmission. Despite this experiment's success as a demonstrator, however, its performance indicators (bit rate, distance, etc.) are not impressive in themselves. Considerable effort and ingenuity have gone on since this demonstration to enhance the technique of quantum key distribution and to turn it into an attractive practical proposition. This effort is the subject of the next section.

3. Quantum key distribution over optical fibre

3.1. *Phase Coding*

Although we have so far concentrated exclusively on polarization, it is not the only property of single photons that can be exploited in a quantum cryptography system. A phase coding scheme can also be adopted as we shall now describe. This scheme is based on the properties of interferometers and the coding is effected by changing the relative phase between the internal arms of the interferometer. An interferometric quantum key distribution system was first proposed by Bennett for his two-state protocol [33]. We shall, however, describe in this section the implementation of the BB84 four-state protocol on interferometric systems. Such quantum interferometric systems have been used to securely transmit keys over optical fibre up to distances of 30 km [6]. A simple communication scheme based on a Mach–Zehnder interferometer is sketched in figure 9 where Alice and Bob each control one half of the interferometer. For the moment let us forget that we wish to implement a quantum key distribution scheme and assume that Alice sends classical pulses of light into the input of her interferometer. The output properties of such a device depend on the interference caused by splitting the beam at the first beam splitter and recombination of the beams at the second. It is the phase difference generated by the relative settings of Alice's and Bob's phase modulators that will determine these output properties. In the schematic version of the interferometer shown in figure 10 we see that Alice's input pulse is split into two by the first beam splitter. The splitting fraction is determined by the reflection coefficient R and transmission coefficient T. These pulses travel around the internal arms of the beam splitter where both Alice and Bob can impose a phase modulation, if desired. Depending on the relative phases chosen and the beam splitter coefficients the pulse

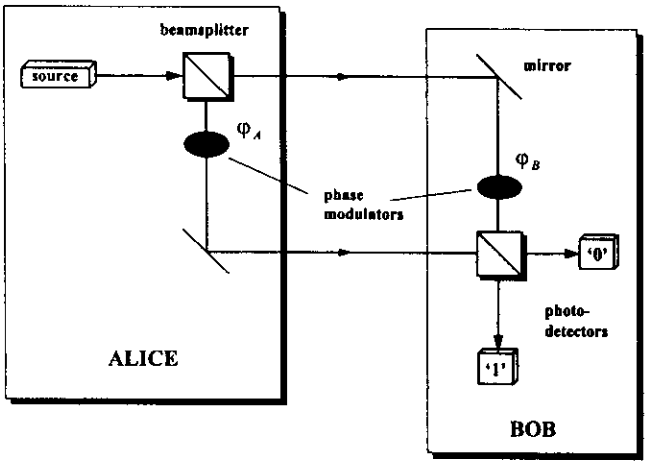
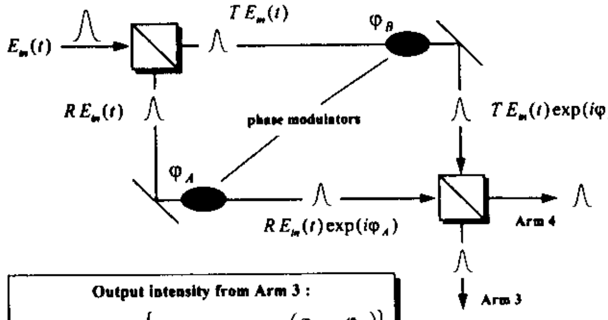


Figure 9. Illustration of the basic interferometer to implement a phase coded BB84 protocol. Alice and Bob each have one half of the interferometer under their control. Alice's phase modulator selects the random coding and Bob's phase modulator selects the measurement basis at random. Each photodetector registers a bit value so that if the photodetector labelled by '1' in the figure registers a count, this is read as a logical 1 for both of the possible basis choices of Bob.



Output intensity from Arm 3 :

$$I_3(t) = |E_{in}(t)|^2\left\{1 - 4|R|^2|T|^2\cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right)\right\}$$

Output intensity from Arm 4 :

$$I_4(t) = 4|E_{in}(t)|^2|R|^2|T|^2\cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$$

Figure 10. The output intensities from the interferometer of figure 9 when a classical pulse is input by Alice. Note that, in general, the intensity is split between the two ouput arms of any beam splitter. Adjustment of the relative phases of the internal arms can lead to switching of the pulse from one of Bob's output ports to the other.

exits the device in either arm 3 or arm 4, or both. For balanced interferometers, that is $|R|^2 = |T|^2 = \frac{1}{2}$, where Bob keeps his phase set at zero and Alice switches hers between zero and π, then Bob will see the pulse emerge in arms 4 and 3 respectively. Thus by choosing the coding scheme phase shift $(0) \equiv 1$, phase shift $(\pi) \equiv 0$, arm $3 \equiv 1$ and arm $4 \equiv 0$, Alice can communicate a binary message to Bob.

The pulse incident on the first beam splitter in figure 10 splits into two. If the incident pulse intensity is $|E_{in}(t)|^2$, then two pulses emerge from the output ports of the beamsplitter with intensities $|R|^2\ |E_{in}(t)|^2$ and $|T|^2\ |E_{in}(t)|^2$ as shown in the figure.† At the phase modulators, Alice and Bob impose a phase shift on their respective portions of the incident pulse. These pulses are recombined at the second beam splitter to give the output intensities shown in the figure. In deriving this result we have made use of the fact that the beam splitters are considered lossless so that $|R|^2 + |T|^2 = 1$, which is just an expression of the fact that the pulse splits between the two possible output ports. We have also included a phase change of $\pi/2$ in the transmitted arm for consistency‡ and have assumed that the two beam splitters of the interferometer are identical in every respect. We can see that the adjustment of the relative phases can result in the output emerging from either arm or both. Such a device can perform a variety of functions from simple switching to logical operations.

Table 2. Coding scheme employed by Alice. The setting of her phase modulator determines the bit value and she has a choice of two ways of coding the same bit

Alice	
Phase setting (degrees)	Bit value
0	0
180	1
90	0
270	1

Suppose now that Alice reduces her input intensity to just one photon per pulse. In simple terms, a single photon incident on a beam splitter cannot go both ways; in other words it cannot be split in the sense that photodetectors placed in both output ports of the first beam splitter will not simultaneously register a count. This can be seen as a consequence of the no-copying theorem for single quanta [27]. If the beam-splitter reflection coefficient is R and the transmission coefficient is T, as in figure 10, then the photon will be found in one arm with probability $|R|^2$ and the other with probability $|T|^2$. As we increase the pulse intensity, we see that this probabilistic rule applied to a multiphoton pulse will lead to a pulse splitting with precisely this intensity ratio. Of course, as with the celebrated two-slit experiment if we decide to interrogate the system to determine in which arm a photon is to be found, we lose the interference, or phase, information.

We shall now concentrate exclusively on balanced interferometers for convenience. The details for the un-

Table 3. Bit measurement scheme employed by Bob. If the photon emerges from arm 3, it is read as a 1 and, if it emerges from arm 4, it is read as a 0. The choice of phase setting gives Bob two different codings for his bit value

Bob	
Phase setting (degrees)	Bit value
0	0 (arm 4) 1 (arm 3)
90	0 (arm 4) 1 (arm 3)

†Of course, in the figure we have shown the effect of the beam splitter on the incident fields. The intensity is proportional to the square modulus of the field. The fields have been shown in the figure to emphasize the interference properties when appropriate phase shifts are chosen in the internal arms.

‡This is just the phase change on reflection observed at dielectric interfaces. Exactly in which arm the phase change is placed is arbitrary, the requirement being that there is a relative phase shift of $\pi/2$ between them. At a fundamental level this phase change is required by the unitarity of quantum mechanics.

balanced case are slightly more complex requiring a consideration of both input ports but such interferometers can also be used for quantum key distribution. In order to use this balanced interferometer to transmit keys, Alice and Bob must agree on a coding scheme. A suitable scheme is for Alice and Bob to choose the bit values shown in tables 2 and 3. So, for example, if Alice sets her modulator at 180°, she records this as a 1. Bob sets his modulator at either zero phase shift or a shift of 90°. He then reads the bit according to which photodetector fires; if the detector in arm 4 fires he reads the bits as a 0. If Alice has chosen the 0°–180° coding to encode her bit and Bob has set his modulator at 90°, then a single photon from Alice will emerge with equal likelihood from either of Bob's output arms and the bit value that Bob reads is probabilistic. It is only when the phase difference between Alice's and Bob's modulator settings is zero or 180° that Bob will achieve a deterministic, and therefore reproducible, result. As before with the polarization coding scheme it is a random choice of coding applied to single photons that ensures the security of the key transfer. Alice and Bob therefore choose randomly, and independently, a modulator setting for each time slot. After the transmission all those time slots where a probabilistic result is expected, that is where the phase difference is 90° or 270° and those time slots where no photon was received by Bob, are discarded. In the remaining time slots, Alice and Bob should share the same random bit sequence.

How does this work as a quantum key distribution scheme? It is not immediately obvious that this kind of interferometric phase coding is equivalent to the polarization coding scheme discussed in the previous section. In the broadest quantum-mechanical terms, quantum key distribution using the BB84 protocol can be achieved using any system spanned by a two-dimensional Hilbert space. Because it is difficult to generate a true single-photon source, a highly attenuated laser diode is usually employed in the experiments [3–6]. This, of course, is not a true single-photon source and the field state is consequently not spanned by a two-dimensional Hilbert space. Let us for the moment assume that Alice does indeed possess a single-photon source. If a single photon is input to the balanced device, what are the outputs at arms 3 and 4? To begin with let us consider the output state from Alice (figure 11). This state is transmitted to Bob and is accessible to Eve. This state can be described by

$$|\psi_{\text{Alice}}(\varphi_{\text{A}})\rangle = \frac{1}{2^{1/2}}\{|1,0\rangle + \text{i}\exp(\text{i}\varphi_{\text{A}})|0,1\rangle\}, \qquad (3.1)$$

where we have used the notation $|1,0\rangle$ to represent the state of the interferometer with the photon in arm 1 and no photon in arm 2. This state is a quantum superposition of the two possible paths that a single photon can take. The states $|1,0\rangle$ and $|0,1\rangle$ form a basis for the one-photon interferometer, that is the interferometer is spanned by a Hilbert space of dimension 2. The states $|\psi_{\text{Alice}}(0°)\rangle$ and $|\psi_{\text{Alice}}(180°)\rangle$ also form an orthonormal basis spanning the space, as indeed do the states $|\psi_{\text{Alice}}(90°)\rangle$ and $|\psi_{\text{Alice}}(270°)\rangle$. However, the operator representing the basis choice 0°/180° is incompatible with the operator representing the basis choice 90°/270°. Technically the two bases are said to be conjugate which is, in some sense, equivalent to saying that they are maximally incompatible. This is precisely the situation obtained with circular and linear polarization. The expansion of the 0° state in the 90°/270° basis is given by

$$\begin{aligned}|\psi_{\text{Alice}}(0°)\rangle = {} & \tfrac{1}{2}(1-\text{i})|\psi_{\text{Alice}}(90°)\rangle \\ & + \tfrac{1}{2}(1+\text{i})|\psi_{\text{Alice}}(270°)\rangle,\end{aligned} \qquad (3.2)$$

so that measurement of the 0° state in the 90°/270° basis will yield a probabilistic result with a 50% chance of reading the bit incorrectly. By selecting a phase modulation of 0° or 90°, Bob is in fact choosing between two measurement bases.

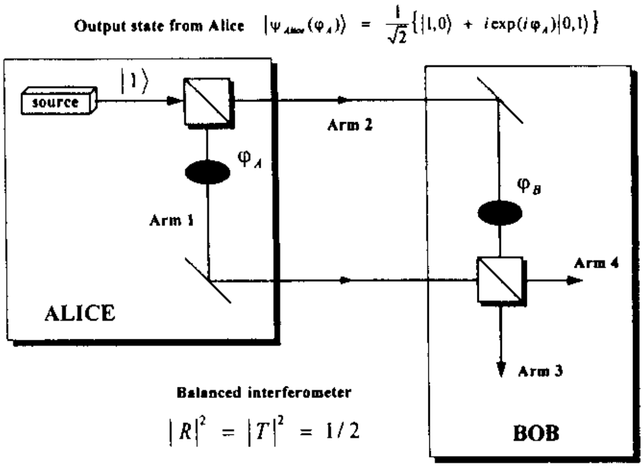

Output state from Alice $|\psi_{Alice}(\varphi_A)\rangle = \frac{1}{\sqrt{2}}\{|1,0\rangle + i\exp(i\varphi_A)|0,1\rangle\}$
source
$|1\rangle$
Arm 2
φ_A
Arm 1
ALICE
φ_B
Arm 4
Arm 3
Balanced interferometer
$|R|^2 = |T|^2 = 1/2$
BOB

Figure 11. Notation and output state from Alice for a single-photon implementation of the interferometric quantum transmission. Note that a balanced interferometer has been assumed. The photon can only be found in one of the internal arms, and not both.

The BB84 protocol with phase coding works exactly as before. Alice chooses the coding 0°/180° or 90°/270° at random and Bob, independently of Alice, selects a measurement basis at random. In the public discussion stage, Alice and Bob discard those time slots where a different phase basis was chosen. Where the same basis was chosen by Alice and Bob, a deterministic result is obtained and Alice and Bob will share an identical sequence of bits after the public discussion in exactly the same way as we have previously described for the polarization coding scheme.

The single-photon interferometer scheme works because the phase shifts of the modulators select between two orthonormal bases. However, it is not strictly necessary that the states used to encode the bits form an orthonormal basis. For example, we could consider using the following coding:

$$\begin{aligned} |u\rangle &\rightarrow 0, \\ |w\rangle &\rightarrow 1, \end{aligned} \tag{3.3}$$

where $\langle u|w\rangle \neq 0$. If we consider the states (3.3) we see that they are not eigenstates of a single operator so that a single measurement, or any sequence of measurements, cannot unambiguously distinguish between them in every case. It is however, possible to find a measurement that will unambiguously distinguish between these states in *some* cases, but not all. An example of such a measurement is given by the projector $1 - |u\rangle\langle u|$. If a non-zero result is obtained, then it can only have come from the state $|w\rangle$. A null result could come from either state. Depending on the outcome of the measurement, therefore, it is possible to distinguish occasionally with certainty between two non-orthogonal states. This property is crucial to the success of the Bennett two-state protocol, or B92, that we shall discuss later [33]. This property is also used in the practical implementations [5, 6] of the four-state phase encoded BB84 protocol as we shall now describe.

Experimentally it is not trivial to produce a source of single photons. In practice, therefore, the output from a laser diode is heavily attenuated so that there is a very low probability of finding more than one photon in any given pulse. An imperfect single-photon source leads to the possibility that Eve can tap off a single photon from a multiphoton pulse and remain undetected, although by keeping the average number of photons per pulse very low this can be made an infrequent occurrence. Such an attack is known as a beam-splitting attack and we shall return to these strategies later. The output from a laser operating well above threshold can be described by a coherent state. The coherent states are important states in quantum optics and the interested reader is referred to Loudon's [34] book for more details on these states and field quantization. Attenuation of coherent states produces a coherent state of reduced amplitude. A coherent state is a minimum-uncertainty state with equal uncertainty in its real and imaginary field components and so can be described by an uncertainty circle on an appropriate phasor plot. The boundary of the circle is calculated from the variances of the operators representing the real and imaginary parts of the field. A single measurement of the amplitude and phase of a field prepared in a coherent state will generate a point on this phasor plot. Many such measurements on an ensemble of identically prepared fields will generate a circular distribution of points centred on the classical amplitude and phase for the field. This pictorial representation of a coherent state and its attenuation are depicted in figure 12. The coherent states form an overcomplete basis and are not an eigenbasis for any Hermitian operator. Consequently they do not form an orthonormal basis. If $|n\rangle$ describes a field state with *exactly n* photons (usually termed the photon number states), then a coherent state of amplitude α is given by the expansion

$$|\alpha\rangle = \exp(-\tfrac{1}{2}|\alpha|^2)\sum_{n=0}^{\infty}\frac{\alpha^n}{(n!)^{1/2}}|n\rangle. \tag{3.4}$$

The mean intensity is given by $|\alpha|^2$ so that equation (3.4) is a Poisson distribution of states with exact numbers of photons. Attenuation of equation (3.4) so that terms of $O(|\alpha|^3)$ are negligible gives the state

$$|\alpha\rangle \approx (1 - \tfrac{1}{2}|\alpha|^2)|0\rangle + |\alpha\rangle + \tfrac{1}{2}\alpha^2|2\rangle. \tag{3.5}$$

This state has a large vacuum component so that such a state incident upon a photodetector would not cause a count most of the time.† When a count is registered, it is much more likely to have originated from the single-photon state than from any state with two or more photons.

Coherent states and single-photon states incident upon beam splitters do not behave in the same fashion. Coherent states are the quantum analogues of classical field states and split at beam splitters in very much the same way as a classical pulse. The previous coding scheme where Alice and Bob were able to select between orthonormal bases by choosing an appropriate phase modulator setting does not apply in the same way here. Let us see how it does work. After the first beam splitter (which we assume to be 50:50 as before) and the phase modulation, the output state of Alice, i.e. the state which travels on to Bob is given by

$$|\psi_{\mathrm{Alice}}\rangle \equiv |\varphi_{\mathrm{A}}\rangle = \left|\frac{1}{2^{1/2}}\alpha\exp(\mathrm{i}\varphi_{\mathrm{A}}), \frac{\mathrm{i}}{2^{1/2}}\alpha\right\rangle. \tag{3.6}$$

The states represented by the choices 0°/180° or 90°/270° are not orthonormal and we have

$$\begin{aligned} |\langle 0^\circ|180^\circ\rangle|^2 = |\langle 90^\circ|270^\circ\rangle|^2 &= \exp(-2|\alpha|^2), \\ |\langle 0^\circ|90^\circ\rangle|^2 = |\langle 0^\circ|270^\circ\rangle|^2 = |\langle 180^\circ|270^\circ\rangle|^2 &= |\langle 180^\circ|90^\circ\rangle|^2 \\ &= \exp(-|\alpha|^2). \end{aligned}$$

If Alice chooses the same coding scheme as before so that the choice 0°/180° represents one way of coding 0/1 and the choice 90°/270° represents the other, then the non-orthonormality of these states means that the bit cannot, in principle, be accurately read all the time. However, as we have hinted at previously, it is possible to distinguish between these states, without ambiguity, some of the time. The interferometer that we have already described is a device that will perform this function. When $|\alpha|^2$ is small, the overlap between the four states is very significant and close to unity. This is due to the large vacuum component in the expansion (3.5). Using the same pictorial representation of the coherent state as before we see in figure 13 a schematic illustration of this significant overlap. Because of this large overlap it is not

†A photodetector performs a measurement of the field's photon number. For the state (3.5), therefore, a measurement of photon number will give the result 0 with probability$(1 - \frac{1}{2}|\alpha|^2)^2$ which is very close to unity. The probability of finding a single photon when making such a measurement is just given by $|\alpha|^2$.

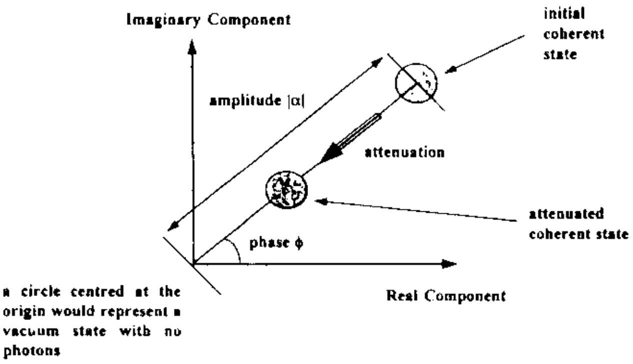

Imaginary Component
initial coherent state
amplitude |α|
attenuation
attenuated coherent state
phase ϕ
a circle centred at the origin would represent a vacuum state with no photons
Real Component

Figure 12. Diagram to represent the evolution of the noise circle for a coherent state under attenuation. Note that the noise circle itself is unchanged but its relative size to the amplitude increases. The relative fluctuations in phase and amplitude therefore increase upon attenuation.

possible to distinguish between the four states generated by the phase settings 0°/90°/180°/270°, in every instance, and it is this indistinguishability that gives the phase-encoded version of BB84 its security when attenuated coherent states are used as approximations to the single photon number state.

The input state to Bob's half-interferometer is given by equation (3.6). This state is also accessible to Eve. However, Bob performs an additional phase modulation which is not accessible to Eve and the state generated after Bob's phase modulation, but before his beam splitter is

$$|\psi_{\mathrm{Alice}}\rangle = \left|\frac{1}{2^{1/2}}\alpha\exp(\mathrm{i}\varphi_{\mathrm{A}}), \frac{\mathrm{i}}{2^{1/2}}\alpha\exp(\mathrm{i}\varphi_{\mathrm{B}})\right\rangle. \quad (3.7)$$

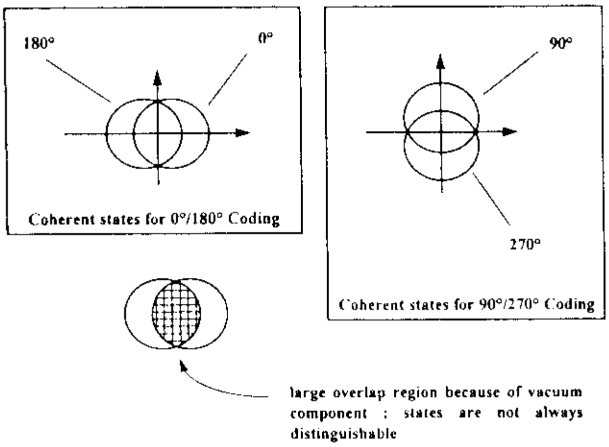

180°
0°
Coherent states for 0°/180° Coding
90°
270°
Coherent states for 90°/270° Coding
large overlap region because of vacuum component : states are not always distinguishable

Figure 13. Schematic representation of the overlap between the coherent states used in the phase coded implementation of the BB84 protocol. This overlap leads to a relatively high error rate as it is difficult to distinguish one symbol from another. However, it is also this overlap that is exploited to guarantee the security of the key distribution.

Table 4. Input states to Bob's photodetectors for the various phase settings chosen. Those phase settings which can never give rise to an unambiguous result are discarded. Alice and Bob each possess one half of a balanced interferometer

Alice	Bob	
Phase setting (degrees)	Phase setting (degrees)	Input tc photodetectors
0	0	$\|0, \mathrm{i}\alpha\rangle$
	90 (discarded)	$\left\|\frac{1-\mathrm{i}}{2}\alpha, \frac{\mathrm{i}-1}{2}\alpha\right\rangle$
180	0	$\|-\alpha, 0\rangle$
	90 (discarded)	$\left\|-\frac{1+\mathrm{i}}{2}\alpha, \frac{1+\mathrm{i}}{2}\alpha\right\rangle$
90	0 (discarded)	$\left\|\frac{\mathrm{i}-1}{2}\alpha, \frac{\mathrm{i}-1}{2}\alpha\right\rangle$
	90	$\|0, -\alpha\rangle$
270	0 (discarded)	$\left\|-\frac{1+\mathrm{i}}{2}\alpha, \frac{\mathrm{i}-1}{2}\alpha\right\rangle$
	90	$\|-\mathrm{i}\alpha, 0\rangle$

The state emerging from Bob's beam splitter and entering the photodetectors is given by

$$\left|\tfrac{1}{2}\alpha[\exp(\mathrm{i}\varphi_{\mathrm{A}}) - \exp(\mathrm{i}\varphi_{\mathrm{B}})], \tfrac{\mathrm{i}}{2}\alpha[\exp(\mathrm{i}\varphi_{\mathrm{A}}) + \exp(\mathrm{i}\varphi_{\mathrm{B}})]\right\rangle. \quad (3.8)$$

The various output states and transmitted bit values are shown in table 4 when Alice and Bob use the same coding scheme as for the single-photon version of this system. Most of the time, because the input intensity of Alice's state is extremely low, Bob's detectors will not register a count, even if Bob were to have perfectly efficient photodetectors. Again this is because of the large vacuum component of these four states. If one of Bob's detectors fires, he records his phase setting and the received bit. If, in the subsequent public discussion, it is found that Bob's phase setting was incorrect, this bit is discarded. If, however, Bob's phase setting is correct and a count is registered, that bit will, for noiseless detectors, also be correct. For example, if we consider the first entry in table 4 we see that there is a vacuum input to the photodetector in arm 3 and a low-intensity coherent state input to the detector in arm 4. The detector in arm 3 will not register a count and the detector in arm 4 will register a count with a probability of approximately $|\alpha|^2$ (remember that $|\alpha|^2 \leqslant 1$). If a count is received and Bob is told that he has the correct phase setting, this can therefore only have come from Alice's state |0°⟩. This is an example of how two non-orthogonal states, the 0°/180° states, can occasionally be distinguished without ambiguity by a single measurement. This does not violate any fundamental principle since, on average, the bits retain their indistinguishability. The last possibility is for both of Bob's detectors to fire simultaneously. This even is of course discarded as this can only arise from an incorrect phase setting on Bob's modulators.

Although it is possible to generate single photons experimentally, it is much easier to produce a close approximation to a single-photon source by heavily attenuating the output from a laser. As we have mentioned, the use of such a strongly attenuated coherent state in a quantum cryptography system allows Eve a particular kind of attack known as a beam-splitting attack. These kinds of attack can at most only obtain a small fraction of the key bits for reasons that we shall now discuss. From equations (3.4) and (3.5) we see that the probability that any given pulse is found to contain one and only one photon is $|\alpha|^2$ and the probability that any given pulse is found to contain two or more photons is $|\alpha|^4/2$. In the experiments $|\alpha|^2$ is about 0·1 so that about 1 in 10 pulses will be found to contain one photon and about 1 in 200 pulses will be found to have two or more photons. In principle, therefore, Eve can try to exploit this by using a beam splitter to tap off a fraction of the signal so that in some instances both she and Bob will receive a photon. If Eve stores this photon until Bob has publicly announced the bases that he chose and then uses this information to perform a measurement in the basis announced by Bob, she will be able to obtain some of the key bits. However, the key will eventually be made up of bits *actually measured* by Bob, and not all these bits will have originated from pulses for which *both* he and Eve received a photon. The events in which Bob receives a photon and Eve receives no photon predominate so that a beam-splitting attack can only ever obtain a small fraction of the key.† This leakage of information to Eve can be accommodated within the privacy amplification procedure [1, 29, 31].

The interferometric quantum key distribution scheme works because, in general, two non-orthogonal states are eigenstates of different incompatible operators. The incompatibility of the operators leads to the non-orthogonality of the states, as well as to an uncertainty relation between the operators. Thus, whilst not wholly analogous to the polarization coding case, the security of this system depends fundamentally on the quantum properties of low-intensity coherent states. In the next sections we shall see how these interferometric schemes are realised in the laboratory.

3.2. *Experimental implementation*

The increasing demand for rapid access to vast quantities of information and the ability to transmit that information will probably require the widespread utilization of the massive capabilities of high-speed all-optical networks. If quantum key distribution is ever to be considered an appropriate solution to security concerns, it must be capable of operating over reasonable distances on such networks.‡ As we shall show in this section, it is currently possible to transmit keys securely over distances of up to 30 km of optical fibre using quantum cryptography. With improved detector technology this distance should increase to around 100 km or more. It is, however, unlikely in the medium term that detectors and fibre technology will improve sufficiently to allow consideration of quantum key distribution over transatlantic distances although there is no fundamental a priori reason why this should not one day be possible. At BT it has been our aim to develop a usable quantum key distribution system that can operate over significant distances in standard telecommunications fibre. Even given that specialized goal there are several technology options that deserve serious consideration. The choice of wavelength and detector, for example, or the choice of phase or polarization coding schemes are issues that need to be addressed. Indeed, as we shall see it is not yet clear as to the optimal protocol to adopt. However, despite these unanswered questions the first BT prototype [5, 6] implemented the BB84 protocol and operated at a wavelength of 1·3 μm utilizing an interferometric system that is capable of securely transmitting keys over distances of up

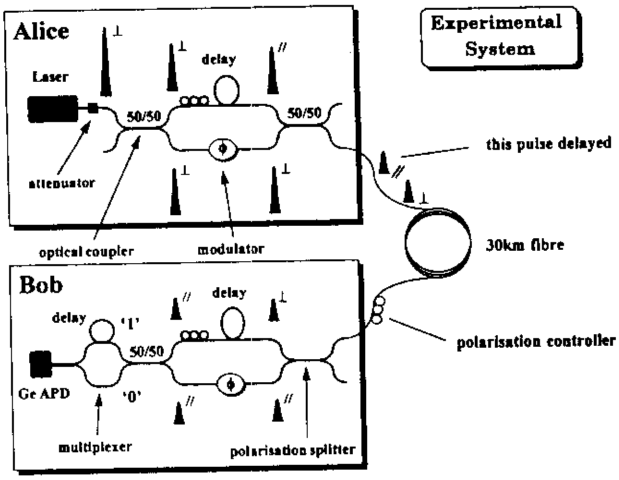


Figure 14. Diagram of the BT prototype quantum key distribution system. To overcome interferometric instabilities that arise in devices of the form shown in figures 9–11 a polarization and time division scheme is used to separate the optical paths. This is achieved by separating the outputs from the first beam splitter–coupler in both time and polarization using a delay stage and polarization controllers. The output from Alice can then travel over a single length of fibre where both output states effectively experience the same environment. It is important to note that interferometric recombination of the pulses occurs only at the final optical coupler.

†This fraction is found to be at most about $|\alpha|^2$ so that, in the experiments, around 10% of the key bits can be obtained by a beam-splitting attack. It should be noted, however, that the success of a beam-splitting attack depends on Eve's ability to store a photon until Bob's measurement basis is revealed. Storage of photons on these time scales is difficult to achieve but we must, nevertheless, allow Eve this capability if we are to give a *guarantee* of security for the key distribution.

‡Of course we do not exclude specialised short-distance applications such as the secure connection between computers in the same building, for example.

to 30 km at data rates of around 1 kbits.† We shall discuss this system in some detail. We have also developed, and are in the process of developing, other prototype systems to enable us to begin to answer some of these important technology questions. Some of the issues that arise from these other systems will also be discussed.

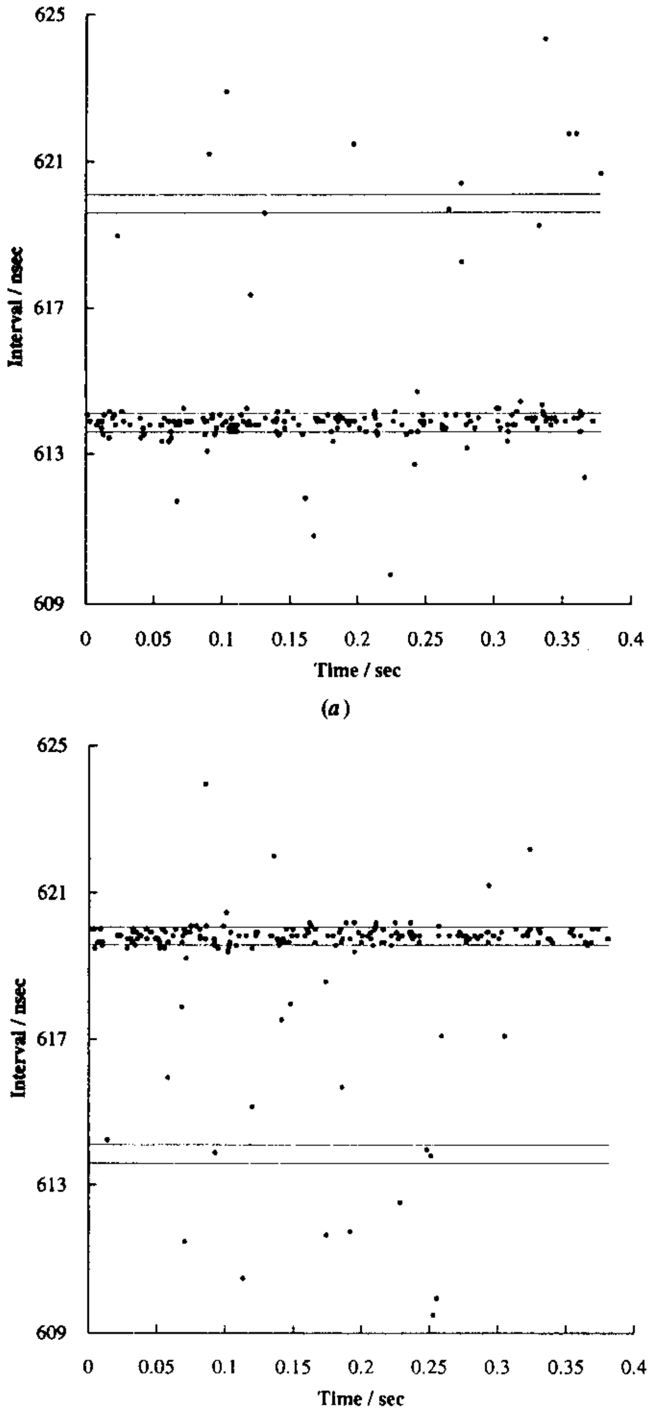
The experimental prototype system [5, 6] shown in figure 14 consists of a 30 km long fibre-based Mach–Zehnder interferometer which operates at a wavelength of 1·3 μm. The laser source is a 1·3 μm wavelength standard semiconductor laser that is gain switched at 1 MHz to produce pulses of 30 ps duration. The pulses from this device are heavily attenuated to a level where the intensity at the input of the transmission fibre, that is Alice's output, is equivalent to 0·1 photons per pulse pair, on average. This attenuated pulse enters an optical coupler (the optical fibre equivalent of a beam splitter) where the pulse splits and one pulse travels through a lithium niobate phase modulator and experiences a phase shift chosen from one of the four possibilities, 0°, 90°, 180°, 270°, at random. The other travels through a polarization controller‡ set to act as a half-wave plate and a delay loop. The half-wave plate rotates the state of polarization of the pulse to its orthogonal state. These two pulses, now with orthogonal polarizations, enter another optical coupler the output of which is fed directly into a length of standard telecommunications fibre 30 km long which is single moded at a wavelength of 1·3 μm. Because of the delay imposed on one pulse these pulses now travel a few nanoseconds apart in this fibre. The time delay between the two pulses must be set so that they both experience the same environmental fluctuations, in other words, the typical fluctuation time scale must be much longer than the time delay between the pulses. In this way the device can be made interferometrically stable over long distances. This kind of interferometer is known as a time division interferometer and it has been used in experiments to reduce the effect of acoustic fluctuations in fibres, known as GAWBS (guided acoustic wave Brillouin scattering), which are an unwanted source of noise in sensitive quantum optical experiments [35].

These pulses form the input to Bob's half of the interferometer where they are spatially separated by the action of a polarization splitter which directs one polarization along one output and the orthogonal polarization along the other. The pulse which did not suffer any phase modulation in Alice's half-interferometer is now given a random phase modulation of 0° or 90° by Bob. The other pulse suffers a time delay of the same magnitude as its partner pulse did in Alice's system and its state of polarization is rotated to match that of the other pulse. These pulses are now recombined at a 50/50 optical coupler where, because they are now temporally coincident with the same polarization, they interfere. Depending on the relative phase settings of Alice and Bob's modulators the resulting output pulse will either emerge in one arm or both. One arm has a further delay loop which allows the temporal separation of the bits so that a 0 value causes the detector, a liquid-nitrogen-cooled germanium avalanche photodiode (APD), to fire first. This allows us to use a single detector where the bits are temporally distinguished. The detector system records each event as a data pair which represents the time elapsed since the start of the key transmission and the time interval value which indicates where the detection occurred within the concurrent laser pulse period. Because photons arriving at the detector originate from the 30 ps optical pulses, they are synchronized with the laser drive and hence give rise to well defined time intervals between the detector event and the beginning of the next laser drive pulse. These time interval values lie within two windows centred at around 614 ns for the 1 output port with the longer path and around 620 ns for the 0 output port. These windows are around 1 ns wide owing to detector timing jitter [36]. In contrast, detector noise mechanisms such as dark counts and after-pulses give rise to counts randomly distributed in time and consequently give rise to random time interval values. After the data transmission is complete, the receiver can use the recorded time interval values to classify each detection event as a 1, a 0 or a noise count. This is shown in figure 15 where an actual data set after discarding instances where different bases were chosen from a typical key transmission is plotted. In this figure the transmission has been separated into two parts for clarity. In figure 15(*a*) we have plotted Bob's results for the time slots where a 1 was transmitted by Alice. Figure 15(*b*) gives the result of those time slots where a 0 was transmitted. By separating the data in this way we can see the extremely low error rates achieved in the experiment.

Typical error rates achieved on this system are around 4% for distances of 30 km and 1·5% for distances of 10 km. These errors arise mainly from the relatively high detector dark count and the less than unity fringe visibility which is of the order of 0·99. However, errors of this magnitude are perfectly acceptable and can be accommodated within the error correction and privacy amplification procedures. As the system length increases and more of the single photons are removed by loss processes in the fibre, the relative proportion of dark counts to data points increases, giving rise to a higher received error rate. With improved detectors and phase modulators both the error rates and the distance of

† We have also investigated prototype systems that operate with source pulse rates of about 100 MHz. Although fully secure key distribution is yet to be demonstrated with this system, the results show that key transmission rates of about 20 kBits should readily be attainable over distances of around 10 km.

‡ These all-fibre devices are made by forming three small consecutive loops in a fibre and allowing the planes of the resultant loops to be adjusted independently. The stress birefringence thereby induced can be used to control the state of polarization of light in a fibre. Such devices are, for obscure reasons, colloquially known as 'bat ears'.



(*a*)

(*b*)

Figure 15. Data obtained from a typical run of the BT prototype system. The transmission data are separated into two plots; in (*a*) we have those time slots where a 1 was transmitted and in (*b*) we have those time slots where a 0 was transmitted. Note the small number of errors in each case.

transmission can be greatly improved. For example, a reduction in the detector dark count rate by a factor of ten would enable a 60 km device to operate at around an error rate of 4%. Apart from the photon-counting electronics associated with the germanium APD and cooling system the components of this system are standard telecommunications components.

The majority of fibre installed worldwide is designed for operation at wavelengths of 1·3 or 1·5 μm where the fibre supports a single spatial mode. Within these two 'windows' the transmission loss of silica fibre reaches a limit set by Rayleigh scattering which is 0·3 dB km^{-1} at 1·3 μm and 0·2 dB km^{-1} at 1·5 μm. With such low transmission losses, signals can propogate for many tens of kilometres before regeneration is required either by means of optoelectronic repeaters or optical amplifiers. A third wavelength region centred on 0·8 μm is also of some interest in telecommunications despite the higher losses of about 2 dB km^{-1} at this wavelength. This is largely due to the availability of cheap optoelectronic components for this wavelength region. However, as we shall discuss, an important consideration is that standard telecommunications fibre supports multiple spatial modes for wavelengths shorter than about 1·2 μm and this can limit system performance. Another issue that influences the transmission distance achievable at a given bit rate is the group velocity dispersion in the fibre. The latter, at 0·8 μm, has a large negative value of − 90 ps nm^{-1} km^{-1}, goes through zero at around 1·3 μm and is positive at 1·5 μm having a value of + 15 ps nm^{-1} km^{-1}. Trade-offs between these factors (and others) that depend on the required system performance determine the choice of 'best' operating wavelength for a conventional telecommunications system. This is likely to be true also for quantum cryptography systems using the same fibre tranmission medium. Consequently, if quantum cryptography is to achieve widespread application, it is important to investigate prototype systems at one or all of these wavelengths to ensure compatibility with existing networks.

Possibly the most important component of a quantum key distribution system is the single-photon detector. There are a variety of commercially available detectors that can operate in single-photon-counting mode, even if not specifically designed for so doing, for various regions of the spectrum. In general, silicon APDs, designed to operate at wavelengths of around 0·8 μm, are at an advanced stage of development whereas germanium and indium gallium arsenide (InGaAs) devices, designed for operation at wavelengths of 1·3 or 1·5 μm are less advanced. Silicon APDs for single-photon counting are commercially available and have a number of attractive features. They have a quantum efficiency of around 30% or higher, they have a low dark count rate of less than 100 counts s^{-1} and they can be thermoelectrically cooled. However, fibre loss and dispersion are greater at 0·8 μm so that transmission distance and bit rates are limited at this wavelength of operation. Germanium and InGaAs devices are at an early stage of development. Photon counting at longer wavelengths has been demonstrated with commercial devices [36, 37] although these were designed for conventional applications and are not yet optimized. In order to operate at longer wavelengths these devices have a smaller bandgap than their silicon-based counterparts and consequently suffer from a relatively high dark count rate. For example, in the case of germanium APD, the device has to be cooled to 77 K to reduce the dark count to a high but manageable level of about 1000 counts s^{-1}. Quantum efficiencies in the region of 10–20% can be attained with gated operation [6]. The operation of germanium-based APDs is limited to upper wavelengths of 1·3 μm with current device designs. Interestingly, single-photon counting has recently been demonstrated at higher temperatures of around 150–200 K using InGaAs APDs, although quantum efficiencies are quite low at the few per cent level. These devices should also operate at 1·5 μm [38] where advantage can be taken of the low fibre loss.

Modulators can also be a source of error if the frequency response of the device is not flat over a large range [5]. This is because of the large-frequency bandwidth of the random signal. Also in a conventional digital transmission system this effect can be reduced by the appropriate choice of 0/1 thresholds in the detection system. However, this is not possible with a single-photon-counting system. Availability and performance of modulators can also affect the choice of coding scheme. For example, phase modulators for fibre systems are standard components that were developed for use in coherent systems. This is not the case for polarization modulators which are more specialized and less commonly available.

Another potential problem from which 850 nm systems suffer is that of modal dispersion. Standard telecommunications fibre is designed to be single mode at 1·3 μm. An input at 850 nm will therefore excite several modes which each propagate down the fibre with a different velocity. However, the 850 nm prototype built at BT Laboratories has successfully overcome this problem and demonstrated that a secure quantum key distribution is possible over 8 km of standard telecommunication fibre at this wavelength [7]. The intrinsic error rates for this prototype are around the 1% level. It is unlikely, however, that 850 nm systems will match the long distances achieved by 1·3 μm systems. At longer distances loss becomes a problem for 850 nm systems and the advantages of superior detectors at this wavelength are quickly lost.

We have come a long way from the initial theoretical ideas. The next two sections take a look at where we might be heading. The first of these describes some other ways that have been invented for the distribution of keys using quantum mechanics. The second, and last, section takes a look farther afield and briefly discusses some recent developments that could have a big impact. Einstein's famous quote, which summed up his distaste for quantum mechanics was that 'God does not play dice with the universe'; in practical quantum cryptography we use God's dice to guarantee the secrecy of our communication.

4. Other protocols

4.1. *Rejected-data protocols*

As we have seen in the implementations of the BB84 protocol, it is a fundamental quantum-mechanical principle that guarantees the security of the quantum key distribution. The principle of complementarity ensures that properties of states represented by incompatible operators cannot be measured with arbitrary accuracy. The Heisenberg uncertainty relation, and similar measurement inequalities [39], place strict limits on our ability to determine these properties. It is important to ask whether other fundamental properties of quantum mechanics can also be used in a secure key distribution system, or indeed whether there is a different way of exploiting the complementarity of quantum mechanics. Since the invention of quantum cryptography there have been several other proposals for secure quantum key distribution. In this section we shall review what seem to us to be the most important of these from a practical viewpoint beginning with the so-called rejected-data protocols (RDPs). Although not termed as such at the time, the first RDP to be invented was the correlated particle protocol, also known as the EPR protocol for reasons that will shortly become clear, in which the key is generated from measurements on pairs of quantum-correlated particles [40]. We shall describe the EPR protocol in section 4.3. Single-particle RDPs [41] were invented in response to a different question and rely on a different quantum property for their security. However, there is an interesting connection between the EPR protocol and single-particle RDPs to which we shall later return.

If we consider a typical quantum key tranmission using a BB84 protocol with polarization coding, then the transmission can split into two groups of data. Those bits sent and received in the correct basis forming one group and those bits sent and received in different bases forming the other group. In the BB84 protocol this latter group is discarded or rejected. We can consider each of these two groups to represent a flow of information. The information flow on a communication channel is derived from consideration of the correlation between the sent and received message. An entropic measure of correlation is used which gives the information content of that correlation, known as the mutual information [42] (see also [43] for the use of information-based measures of correlation in quantum optics). In the first group, consisting of the raw key data, we would expect, in the absence of noise sources, a perfect correlation between the sent and received data. In other words we would expect a maximal information transmission in this set. In the second group we expect no correlation and therefore no information transmission because for each data pair a different conjugate basis was used to transmit and receive respectively. In the BB84 protocol Alice and Bob examine a randomly chosen sample from the raw key data and check for deviations from the expected high degree of correlation. This procedure allows them to estimate an error rate and to determine whether a secret key can be established. We shall call the BB84 protocol, and other such protocols, 'sacrificial' in the sense that some potential key data needs to be sacrificed to guarantee the security. The data in the other group, the rejected data, are discarded in the BB84 protocol. However, when they are using conjugate bases, Alice and Bob expect this rejected-data set to be uncorrelated. An eavesdropper can also cause a deviation from this expected lack of correlation. Instead of discarding this data, therefore, Alice and Bob should examine these rejected data for evidence of unusual correlation. In information theory terms an increased correlation between sent and received data is equivalent to an increased information flow[†] so that an eavesdropper can, in this sense, cause an information flow on the quantum channel where none was expected.

Under what circumstances can we expect an eavesdropper to cause such an information flow on the rejected data? Let us consider what happens when Alice and Bob use the quantum channel. For each time slot Alice prepares a quantum particle in a definite state and transmits this to Bob. This state preparation can be thought of as being nothing more than the operation of the quantum state filter that we saw in section 2.1 where Alice simply selects between filters at random. Bob's measurement can also be thought of in these terms whereby the result of any measurement can be thought of as due to the application of the relevant quantum state filter. We saw that an intermediate measurement, between Alice and Bob, can be detected by them only if the intermediate measurement can be generated from a filter that represents an incompatible property to *both* of the properties represented by Alice's and Bob's filters. The BB84 protocol works because, when Alice and Bob use the same kind of filter, in other words when they choose the same basis, any intermediate measurement in an incompatible basis is automatically incompatible with both Alice's and Bob's basis. If we let $J(\hat{A}, \hat{B})$ be the information flow between Alice and Bob when they use the bases represented by the operators $\hat{A}$ and $\hat{B}$ respectively, and $J_{\mathrm{E}}(\hat{A}, \hat{B})$ be the information flow in the presence of Eve we can define [41] a channel disturbance parameter ξ which gives the degree of disturbance cased, by the eavesdropper, to the information flow on the channel in those instances where Alice and Bob have used the bases represented by the operators $\hat{A}$ and $\hat{B}$. We divide by the maximal information flow possible, labelled by the subscript max, to normalize the variation in this parameter to ± 1. The channel disturbance parameter is then given by

$$\xi(\hat{A}, \hat{B}) = \frac{J_{\mathrm{E}}(\hat{A}, \hat{B}) - J(\hat{A}, \hat{B})}{J_{\max}(\hat{A}, \hat{B})}. \tag{4.1}$$

When Eve is absent, so that $J_{\mathrm{E}} = J$, this parameter is zero, for any choice of basis by Alice and Bob. Eve's strategy, therefore, should be to adopt a measurement procedure that fools Alice and Bob into thinking she is not there, i.e. one which causes least disturbance to the channel. Alice and Bob expect to obtain the maximal information transmission when they are using the same basis, i.e. when $\hat{A}$ and $\hat{B}$ are in fact the same operator. If Eve attempts to listen to these transmissions in the wrong basis, she will inevitably cause errors, thereby causing J_{E}, the information flow between Alice and Bob in the presence of Eve, to decrease. The channel disturbance parameter then becomes negative, indicating that Eve's intervention causes a loss of information, i.e. a loss of correlation. Similarly, if Alice and Bob are using conjugate bases so that they expect no correlation between sent and received data and Eve's intercepts in a mutually incompatible basis, she will, in general cause there to be fewer errors (she cannot, of course, increase the number of errors!), which increases the correlation and therefore is equivalent to the creation of an information flow between Alice and Bob. In this case, ξ is positive, indicating the creation of information by Eve's attack.

This information-theoretical treatment of the disturbance caused by eavesdropping leads to a simple pictorial representation of quantum key distribution systems that can yield useful insights [26]. Let us call the channel between Alice and Bob 'reducible' if Eve chooses the same basis as *either* Alice or Bob. On a reducible channel, Eve is transparent to Alice and Bob and cannot be detected. If Eve

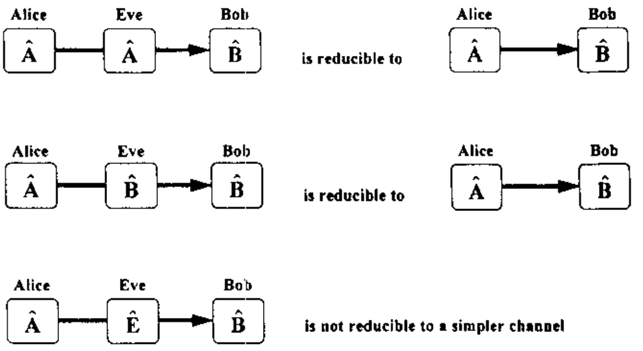


Figure 16. Diagram representing reducible and irreducible channels. It is only on irreducible channels that the effect of Eve can be detected.

[†] Of course, it would be extremely unlikely that an eavesdropper's intervention would cause an intelligible message to flow. Information theory provides a measurement of the degree of correlation between the input and output ends of a communication channel; in other words it provides a measure of how accurately a bit sequence can be transmitted and at what rate. It does not specify that that bit sequence should have meaning. A perfect channel, in information theory terms, would still obey the maxim 'garbage in, garbage out' but it would be faithfully transmitted garbage.

chooses a basis incompatible with *both* Alice's and Bob's, we call the channel 'irreducible' and the channel disturbance parameter cannot be made equal to zero on such channels. A reducible channel is exactly the same, as far as Alice and Bob are concerned to a channel with Eve absent; hence the three nodes can be reduced to two and the channel disturbance parameter is zero. Examples of reducible and irreducible channels are depicted in figure 16. However, because ξ is a statistical parameter, Eve only needs to adopt a strategy such that, *on average*, this parameter is zero. For example, suppose that Eve's measurement in one basis causes a positive correlation between Alice's and Bob's data where none was expected and measurement in another basis yields an equal amount of negative correlation.† In order to avoid detection on this data set Eve should simply switch randomly between these two measurement bases; the negative and positive correlation will, on average, cancel, leading to an uncorrelated data set [44].

Let us denote the entire set of Eve's measurements by

$$\{\hat{\mathbf{E}}\} \equiv \{\hat{E}_1, \hat{E}_2, \hat{E}_3, \ldots, \hat{E}_k, \ldots\}. \qquad (4.2)$$

Depending on her overall strategy, Eve will select a measurement basis represented by an operator from this set for each transmission time slot that she wishes to intercept. There will be a certain probability distribution associated with her choice. We can represent the effect of Eve's strategy on the information received by Bob as a single operator. The condition for Alice and Bob to detect Eve on any particular rejected-data channel can now be generalized from equation (2.10) so that the operator representing Eve's strategy must be incompatible, *on average*, with both Alice's and Bob's observables. A channel where this is the case is said to be irreducible. Of course, for sacrificial channels where perfect correlation is expected, and for perfect channels and detectors, even a single deviation is sufficient to alert Alice and Bob. Thus, although Eve's strategy will not change the average number of agreements between Alice and Bob, more sophisticated statistical tests reveal her presence. On a channel, for example, where Alice and Bob expect a 10% deviation from perfect agreement, Eve must choose an appropriate strategy, to reproduce these statistics. With this generalization we can now state a useful general theorem for the detection of an eavesdropper on a quantum channel. This theorem [26] states:

An eavesdropper can only be detected on an irreducible channel.

An immediate consequence of this statement is that a minimum of two incompatible operators, or bases, are needed to guarantee the security of the channel. A second consequence is that a RDP can only be made secure if at least three incompatible observables are chosen by either Alice or Bob. It is always possible to avoid detection on the rejected data if just two incompatible bases are chosen so that only sacrificial protocols can be made secure with this choice. These consequences of the above theorem are easy to see from simple diagrams as in figure 16 where Eve uses a single measurement basis, and in figure 17 where we show pictorially why a RDP with more than two bases can be made secure against Eve's range of strategies. In figure 17, Alice chooses three incompatible bases and Bob two. We see that, although it is possible for Eve to remain undetected on selected channels if she chooses her operator set carefully, it is not possible for her to choose an operator set which will achieve this for all the rejected-data channels simultaneously. Of course, Alice and Bob must select the operators carefully too! Various specific examples of RDPs and their security have been discussed in [43, 44] and examples of eavesdropping strategies to equalise positive and negative correlation are discussed in [44] and shown to be ineffective against a suitably chosen three-basis rejected-data protocol.

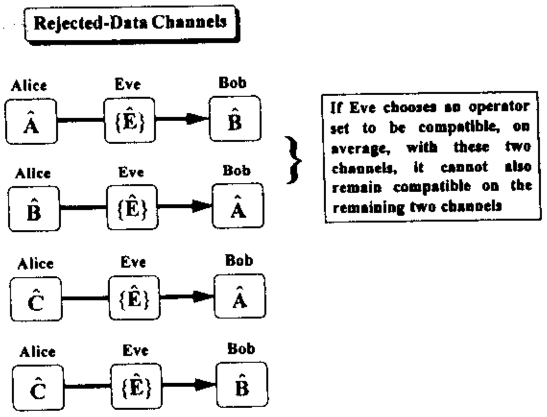

Rejected-Data Channels
Alice
Eve
Bob
Â
{Ê}
B̂
Alice
Eve
Bob
B̂
{Ê}
Â
Alice
Eve
Bob
Ĉ
{Ê}
Â
Alice
Eve
Bob
Ĉ
{Ê}
B̂
If Eve chooses an operator set to be compatible, on average, with these two channels, it cannot also remain compatible on the remaining two channels

Figure 17. The rejected-data channels for a three-alphabet RDP. Eve cannot recreate the statistics on all of these channels with any possible measurement strategy.

Examination of the rejected data can substantially limit the range of strategies that Eve could have employed. For example, if the rejected data are examined in the BB84 protocol and are found to exhibit no spurious extra correlations, this would mean that Eve has attacked in a particular way (or not at all, of course) so that certain measurement strategies could then be discounted. A much more accurate estimate of Eve's expected information gain from the eavesdropping can thereby be established. Obviously, as is evident from the above theorem, it would not be a secure strategy to rely on the rejected data alone when using only two bases as in the BB84 protocol. However, why throw the extra data away without analysis? The entire rejected-data set can be analysed without compromising any security as this data will never be used to form part of the key. This is

†Mutual information does not distinguish between positive and negative correlation so that an increase in negative correlation, or anticorrelation, is equivalent to a flow of information on the channel.

a nice feature of a RDP approach; it can be used in conjunction with sacrificial protocols such as BB84. It is not an either/or choice of protocol. The two types of collected data, rejected and raw key data, are completely independent and can be processed independently. BB84 can therefore be enhanced by the simple expedient of analysis of the rejected data. Of course, if you wanted to be sure that an eavesdropper could be detected on the rejected data alone, you would need to choose three incompatible bases. However, even with this choice you are still free to perform a sacrificial protocol, i.e. to examine some potential key data publicly, to assess the security. This sacrificial test can be performed at any stage after the data acquisition and is independent of any rejected-data tests. The principal benefit of rejected-data type protocols will probably turn out to be as an enhancement to sacrificial protocols and as a technique for providing a more accurate estimate of an eavesdropper's likely information. Given the bit rates achievable in the prototypes and the fact that keys for cryptographic purposes do not, usually, need to be more than a few hundred bits long, it does not seem to us to be likely that RDPs will ever be used to guarantee security on their own. When thousands of bits can be transmitted and processed per second, the most sensible course of action for Alice and Bob is to use every available technique to esimate the possible information leakage to Eve.

4.2. *Two-state protocols*

We have seen that the BB84 protocol requires four states: two to each conjugate basis. It is, however, possible to use just two non-orthogonal quantum states for secure quantum key distribution. This technique was invented by Bennett [33] and is sometimes known as the B92 protocol. We have touched on the use of non-orthogonal states in section 3.1 where we saw that such states can give security in an interferometric version of BB84. The two-state protocol can also be implemented interferometrically [33] and a prototype system is under development [9, 45]. The two states in the B92 protocol can be viewed as being single members of two incompatible bases. Let us consider two states $|\Lambda_0\rangle$ and $|\Omega_0\rangle$ which are members of two incompatible bases with the eigenvalue relationships

$$\hat{\Lambda}|\Lambda_j\rangle = \lambda_j|\Lambda_j\rangle \text{ and } \hat{\Omega}|\Omega_k\rangle = \omega_k|\Omega_k\rangle. \tag{4.3}$$

Now, if we consider the Hermitian projection operators given by

$$\hat{P}(\Lambda_0) = 1 - |\Lambda_0\rangle\langle\Lambda_0| \text{ and } \hat{P}(\Omega_0) = 1 - |\Omega_0\rangle\langle\Omega_0|, \tag{4.4}$$

these have the following eigenvalue relationships:

$$\begin{aligned} \hat{P}(\Lambda_0)|\Lambda_j\rangle &= \begin{cases} |\Lambda_j\rangle & (\text{if } j \neq 0), \\ 0 & (\text{if } j = 0), \end{cases} \\ \hat{P}(\Omega_0)|\Omega_k\rangle &= \begin{cases} |\Omega_k\rangle & (\text{if } k \neq 0), \\ 0 & (\text{if } k = 0). \end{cases} \end{aligned} \tag{4.5}$$

Suppose that Alice transmits to Bob one of the states $|\Lambda_0\rangle$ and $|\Omega_0\rangle$ without Bob knowing which one. Because these states are non-orthogonal, there is no single experiment that will unambiguously distinguish between them in every instance. Suppose Bob has chosen to make a measurement of the observable represented by the projector $\hat{P}(\Omega_0)$ and Alice has transmitted the state $|\Omega_0\rangle$. The result of Bob's measurement will be zero. Suppose, however, that Alice had transmitted the state $|\Lambda_0\rangle$; the outcome of Bob's measurement would then be probabilistic. The state $|\Lambda_0\rangle$ can be expanded in the Ω basis as

$$|\Lambda_0\rangle = \sum_{k=0} |\Omega_k\rangle\langle\Omega_k|\Lambda_0\rangle, \tag{4.6}$$

so that the probability of obtaining the value of zero when this state is transmitted is the probability of obtaining the state $|\Omega_0\rangle$ which is just $|\langle\Omega_0|\Lambda_0\rangle|^2$. All other instances will yield a value of unity and the probability that this occurs is simply given by $1 - |\langle\Omega_0|\Lambda_0\rangle|^2$. If Bob obtains a value of unity as a result of his measurement of the projector $\hat{P}(\Omega_0)$, he knows that this can only have come from the state $|\Lambda_0\rangle$ and not from the state $|\Omega_0\rangle$. A similar situation occurs when Bob chooses to measure the other projector $\hat{P}(\Omega_0)$, where a value of unity, obtained with the same probability of $1 - |\langle\Omega_0|\Lambda_0\rangle|^2$, can only have occurred from an incident state of $|\Omega_0\rangle$. If Alice and Bob choose to label one of these states as a logical 1 and the other as a logical 0, they can establish a random bit sequence by randomly switching between bases, independently, as before. If a null, or zero, result is obtained, this time slot is discarded. Bob simply informs Alice publicly in which time slots he received a non-zero result and the bits transmitted in those time slots form the key. The error–eavesdropper test is performed, as before, by publicly comparing a randomly chosen subset of the bit values. The probabilities and measurement outcomes are shown in table 5. We see from

Table 5. The probabilities for the various outcomes in the two-state protocol

	Bob	
Alice sends	Measures	Reads
$\|\Omega_0\rangle$ bit value 1	$\hat{P}(\Omega_0)$	Null result with probability 1 (discarded)
	$\hat{P}(\Lambda_0)$	Null result with probability $\|\langle\Omega_0\|\Lambda_0\rangle\|^2$ (discarded) 1 read with probability $1 - \|\langle\Omega_0\|\Lambda_0\rangle\|^2$
$\|\Lambda_0\rangle$ bit value 0	$\hat{P}(\Lambda_0)$	Null result with probability 1 (discarded)
	$\hat{P}(\Omega_0)$	Null result with probability $\|\langle\Omega_0\|\Lambda_0\rangle\|^2$ (discarded) 0 read with probability $1 - \|\langle\Omega_0\|\Lambda_0\rangle\|^2$

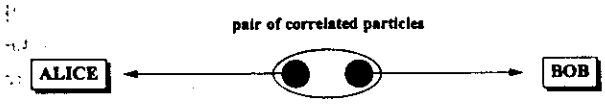


Figure 18. Schematic illustration of the transmission of correlated particles to Alice and Bob in the EPR protocol.

the table that any null result is discarded so that the overall probability that a transmission from Alice is useful is just $\frac{1}{2}(1 - |\langle\Omega_0|\Lambda_0\rangle|^2)$. If the two states are from conjugate bases this fraction is just $\frac{1}{4}$. The key is established from those useful bits received by Bob. Bob just informs Alice which time slots to use. As this is a sacrificial protocol, a random sample of the raw key data is checked for errors and reconciliation and privacy amplification are performed as before.

4.3. *The Einstein–Podolsky–Rosen protocol*

In 1992 a radically different protocol based on the properties of quantum-correlated particles was proposed [40]. The security of the key transmission relies on the peculiar nature of quantum correlation. The statistical test that is performed to assess the integrity of the transmission is exactly that suggested by Bell [46] to distinguish between quantum mechanics and alternative 'classical' theories known as local hidden-variable (LHV) theories. The apparently paradoxical nature of quantum correlation was first highlighted in a celebrated paper by Einstein, Podolsky and Rosen (EPR) [47]. It was shown there that a pair of correlated particles, spatially separated and in separate light cones, could produce what seemed to be a 'spooky action at a distance'. The argument was advanced that quantum mechanics was incomplete and that there must be some 'hidden variables', inaccessible in experiments, that govern the quantum evolution. This problem was, by and large, not a central concern until Bell [48] showed in 1964 that there was in fact an experimentally testable difference between quantum mechanics and these hidden-variable theories.† This test, originally designed to distinguish between competing theories, becomes the basis of the security in the EPR protocol of Ekert [40]. In this protocol the eavesdropper plays the role of a hidden variable and disturbs the quantum nature of the correlation thereby revealing her presence. The statistical test takes the form of an inequality known as the Bell inequality. Classical LHV theories should always satisfy this inequality; quantum mechanics, however, can violate it.

In the EPR protocol, for each time slot, one of a pair of correlated particles is sent to Alice and its partner to Bob. This is sketched in figure 18. Alice and Bob make random measurements, as we shall explain shortly and, after public discussion, separate their results into two groups; those where the same basis was used to form one group and those where different bases were used to form the other. The former group is used to establish a secret key. The latter group is publicly compared, and Alice and Bob use these data to test publicly for a violation of the Bell inequality. If a violation is found, they can infer that there has been no eavesdropping. If, on the other hand, the Bell inequality is satisfied this implies the presence of hidden variables or the eavesdropper. A nice feature of this system is that the key does not actually exist in any way until Alice or Bob make a measurement. In the BB84 protocol the key exists embedded in the data that Alice transmits even though which bits are to be used is decided later and the security comes about because an eavesdropper does not know which measurement to perform. In the EPR protocol when a measurement is made on one of the particles that it introduces, in effect, a definite bit value for that particle and its partner. Until that measurement is made, however, neither of the particles can be said to be individually in a particular state.

Let us consider a pair of photons labelled with the subscripts 1 and 2 having correlated linear polarizations. Quantum-mechanically such a state can be represented by

$$|\psi_{12}\rangle = \frac{1}{2^{1/2}}(|0°\rangle_1 \otimes |90°\rangle_2 - |90°\rangle_1 \otimes |0°\rangle_2), \qquad (4.7)$$

so that, if one particle is measured and found to be in a state of horizontal polarization, that is $|90°\rangle$, the other particle will be found to be in the orthogonal state, namely $|0°\rangle$. Let us now suppose that measurements are made on each particle independently and that each measurement is chosen at random from one of three possibilities, namely measurement of linear polarization defined by the axes at angles 0°, 30° and

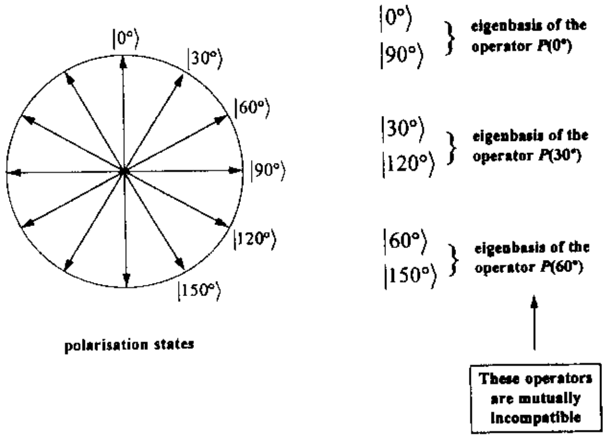


Figure 19. Diagram to show the possible polarization bases used in the EPR protocol. The three bases are chosen so that the eigenstates bisect the circle equally. A maximal violation of the Bell inequality is observed with this choice of polarization bases.

†Specifically, this distinction only exists between LHV theories and quantum mechanics. If the hidden variables are allowed to influence the behaviour of a quantum system in a non-local way, then the predictions of quantum mechanics can be reproduced by these non-local hidden-variable theories.

60°. The polarization states forming the eigenbases of the operators representing measurements at these angles are sketched in figure 19. Each choice of measurement angle denotes a distinct choice of basis. Let us denote the operator representing a measurement of one of these polarizations by $P(X^0)$ where X can take one of the values 0, 30 or 60. After many such measurements on a sequence of particles prepared in the state (4.7) we should now have two sets of data: those instances where the same operator was chosen and those instances where different operators were chosen. This second data set is now analysed and the following quantity, B, is formed:

$$B = 1 + D(30°, 60°) - |D(0°, 30°) - D(0°, 60°)|, \quad (4.8)$$

where, for example, the quantity $D(0°, 30°)$ is the difference between the probability of obtaining a different state and the probability of obtaining the same state in the measurements on particles 1 and 2 when the operator $P(0°)$ was used for one measurement and $P(30°)$ was used for the other. Bell showed that any theory based on assumptions of locality and so-called hidden variables had to satisfy, in general, the inequality $B \geqslant 0$ for any choice of three measurement angles. This is the form of Bell's original inequality although other versions have been given. For the three angles given, the quantum mechanical prediction is that $B = -\frac{1}{2}$ which is a clear violation of the inequality.

Suppose now that Alice and Bob both receive, for each time slot, a photon from a correlated pair. For each time slot they choose, independently and at random, one of the three measurements of linear polarization characterized by the angles 0°, 30° and 60°. The first state in any basis pair, that is the $|0°\rangle$, $|30°\rangle$ and $|60°\rangle$, are labelled as 0 bit values, and their partner states in the basis, $|90°\rangle$, $|120°\rangle$ and $|150°\rangle$, respectively, are labelled as 1 bit values. Because the state (4.7) is anticorrelated, Bob (or Alice, but only one of them) must perform a bit flip on his bits to be consistent with this coding. The key bits are established whenever Alice and Bob choose the same basis. In these instances the correlation between the particles ensures that the same bit value, after Bob's bit flip, is recorded by both of them. This is quite a remarkable property of particles correlated in a way described by equation (4.7). It is this seeming 'action at a distance' whereby the measurement of one of the particles, thereby collapsing the wavefunction and projecting the particle into a definite state, that determines the state of its partner. Thus, suppose that Alice measured a linear polarization represented by the operator $P(30°)$ and obtained the result $|120°\rangle$; she records the bit value 1. If Bob also chose to measure polarization along this axis, he would obtain the state $|30°\rangle$ which after his bit flip is read as a 1 also. This projection of the correlated particle pair into a definite state is important as we shall see in the next section. For time slots where Alice and Bob used different operators the data set obtained is subjected to the statistical test outlined above which amounts to a test for hidden variables. A small randomly chosen subset of the key data should also be publicly compared to assess any residual error rate for the purposes of reconciliation and privacy amplification.

Interferometric versions based on Franson's [49] interferometer, developed to display violations of the Bell inequality, have been proposed [50]. These experiments, which have not yet demonstrated key transmission [51] have not been as successful as the single-particle implementations of BB84 and B92 [3–9, 45]. This is partly due to the difficulty of handling correlated particles and the difficulty of finding detectors efficient enough to demonstrate true violations of the Bell inequality. However, it should only be a matter of time before a prototype quantum key distribution system based on correlated particles is operational. We have seen that, because the EPR protocol is a rejected-data protocol, the raw key data can also be used to assess the integrity of the channel. Thus an adapted BB84 using six states instead of the usual four can be used in conjunction with this EPR protocol. As a final twist, the correlated particles can be used to implement the BB84 protocol in full by simply restricting the measurement set to just two conjugate operators [52]. This, in effect, makes use of the correlated particles as an elaborate form of state preparation. We shall take this idea further in the next section.

4.4. *The Einstein–Podolsky–Rosen protocol with single particles*

We have seen how correlated particles can be exploited in a secure quantum key distribution scheme. We now show how it is possible to use precisely the same EPR protocol, with the same level of security, *using only single particles* [53]. This leads to an interesting speculation concerning rejected-data protocols in general.

Before we describe why this works, it is essential to note two things. Firstly, the Bell inequality is derived from rather general assumptions and its violation, or otherwise, does not depend on any notion of which measurement was performed first. For example, if Alice performs her measurement well before Bob's measurement, thus projecting the particle that travels on to Bob into a definite state, and if Bob measures randomly and independently of Alice, as before, they will still see a violation of the inequality for quantum-correlated particles. Thus, although the inequality has been used to probe questions of non-locality, it is not strictly necessary for the two particles to lie outside each other's light cone in order to see a violation of the inequality. Secondly, Alice's measurement can be seen as a kind of state preparation. This is illustrated in table 6 where we see that Alice's measurement, performed before Bob's, determines the state of the photon that Bob receives. Thus Alice could maintain the correlated particle source in her laboratory and make random chosen measurements on one particle, as described, and send

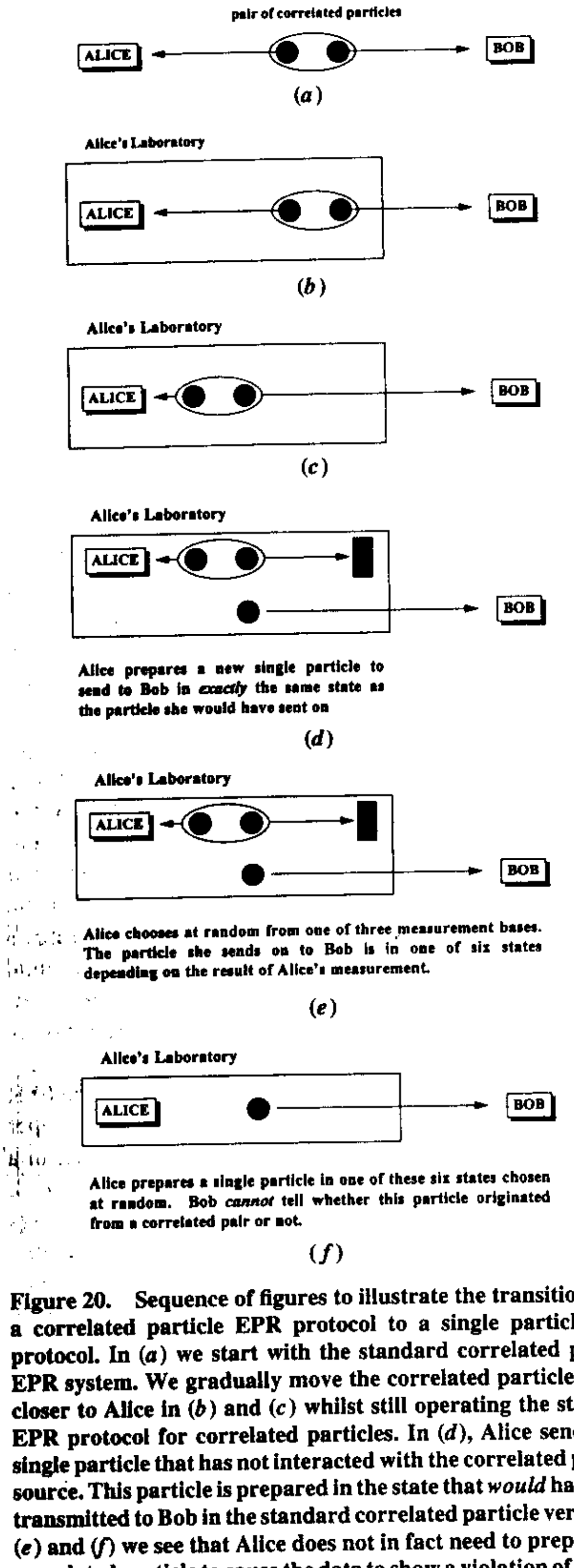
Table 6. The state received by Bob when Alice performs a prior measurement on her particle

Alice's randomly chosen measurement basis (each measurement can give rise to one of two results)	Result of Alice's measurement (each result occurs with 50% probability)	State that Bob receives after Alice's measurement (a definite state is received after Alice's measurement)
$P(0°)$	$\|0°\rangle_1$	$\|90°\rangle_2$
	$\|90°\rangle_1$	$\|0°\rangle_2$
$P(30°)$	$\|30°\rangle_1$	$\|120°\rangle_2$
	$\|120°\rangle_1$	$\|30°\rangle_2$
$P(60°)$	$\|60°\rangle_1$	$\|150°\rangle_2$
	$\|150°\rangle_1$	$\|60°\rangle_2$

the partner particle on to Bob. Alice would, of course, know the result of her measurement and would therefore know the precise state sent on to Bob. Bob would randomly and independently of Alice choose a measurement basis and would record the results of his measurements. If Alice and Bob subsequently compare data, they would notice a violation of the Bell inequality on their rejected-data set.

Let us now consider the sequence of events sketched in figure 20. We start in figure 20(a) with a pair of correlated photons, one of which is sent to Bob and the other to Alice. Alice and Bob make simultaneous, independent and randomly chosen measurements of the polarizations. They record their results and discuss those in which they chose a different polarization to measure. When they form the quantity B given by equation (4.8), they find it is negative in agreement with the predictions of quantum mechanics. In other words, they find that the Bell inequality is violated. In figure 20(b), nothing changes except that the photons both originate in Alice's laboratory (which for the purposes of this sequence of thought experiments we assume to be rather long!). Alice and Bob will, of course, observe a violation of Bell's inequality in this situation. Let us now suppose that the two-photon source is much closer to Alice as shown in figure 20(c). Alice makes her measurements on one of the photons and allows its partner to travel out of her laboratory to Bob. As we have seen, the violation of the mathematical expression known as Bell's inequality does not depend on the sequence in which the measurements on the two particles are made so that, when Alice and Bob compare data, they will still observe a violation of the inequality. Let us now suppose that Alice prevents the partner photon from leaving her laboratory and substitutes another photon, prepared in exactly the same state as the partner photon, which then leaves her laboratory and travels on to Bob as depicted in figure 20(d). Comparison of the data between Alice and Bob will still reveal a violation of the Bell inequality even though the two photons are now correlated by a deliberate act of state preparation. There is no experiment that Bob can perform that will allow him to determine whether the photon that he has received has originated from a correlated source or is simply a single photon prepared in a known state. After Bob's measurement, Alice can tell Bob both the measurement basis and the result received but, if she chooses not to reveal the exact nature of her photon source, Bob cannot uncover it from the data. Now, because Alice is choosing a measurement basis at random, this has the effect of preparing Bob's photon in a randomly chosen state from one of the six possible polarization states shown in table 6. Alice could therefore simply prepare a sequence of single photons each photon being in one of these states chosen at random and send it on to Bob, recording the state of each individual photon. This is shown in figure 20(f). Bob performs a randomly chosen measurement for each photon and Alice and Bob subsequently compare data. They will still observe a violation of the Bell inequality on their rejected-data set. Physically, of course, Bob cannot distinguish between a photon prepared in a random state and a photon from a correlated pair so that a violation of the inequality is observed in the absence of an eavesdropper and the inequality is restored in an eavesdropper's presence. In this way we can achieve EPR security by using *single photons*!

It is easy to see in the correlated photon version of the EPR protocol that the security arises from an eavesdropper behaving like a hidden variable. The same is still true, in a sense, for the single-photon version of this protocol. However, in the single-particle version the security arises from complementarity and the Bell inequality, which in this physical situation has nothing to say about non-locality, can be derived from the quantum rules for transition probabilities. An excellent derivation of this has been given by D'Espagnat [54]. In quantum mechanics, possible trajectories are described by probability amplitudes and not classical probabilities. These amplitudes can interfere as we saw in section 2.1. An eavesdropper's intervention causes these possibilities to collapse onto an actuality so destroying the interference. It is in this sense that an eavesdropper acts as a hidden variable for single-particle versions of the EPR protocol and restores classical behaviour. It is an interesting speculation that a rejected-data protocol can only be made secure, in general, if the bases chosen lead to a violation of a suitably chosen Bell inequality [44]. In the next section we shall continue in speculative vein and examine some future technologies and their implications.



Alice prepares a new single particle to send to Bob in *exactly* the same state as the particle she would have sent on

Alice chooses at random from one of three measurement bases. The particle she sends on to Bob is in one of six states depending on the result of Alice's measurement.

Alice prepares a single particle in one of these six states chosen at random. Bob *cannot* tell whether this particle originated from a correlated pair or not.

Figure 20. Sequence of figures to illustrate the transition from a correlated particle EPR protocol to a single particle EPR protocol. In (*a*) we start with the standard correlated particle EPR system. We gradually move the correlated particle source closer to Alice in (*b*) and (*c*) whilst still operating the standard EPR protocol for correlated particles. In (*d*), Alice sends on a single particle that has not interacted with the correlated particle source. This particle is prepared in the state that *would* have been transmitted to Bob in the standard correlated particle version. In (*e*) and (*f*) we see that Alice does not in fact need to prepare any correlated particle to cause the data to show a violation of the Bell inequality. By establishing a correlation between her state preparation and Bob's measurement in this way, Alice can implement the EPR protocol with single particles.

5. Future directions

5.1. *Quantum key distribution on optical networks*

Quantum key distribution is an intriguing and exciting possibility. However, its implementation on point-to-point links, as we have so far discussed, is only of limited applicability. If quantum key distribution can be made to work on the next generation of optical networks its potential impact could be considerable. At BT we have developed several techniques that will allow the implementation of these quantum techniques on optical networks [55, 56]. For the purposes of brevity we shall consider here only one network configuration, that of a branched or tree configuration network [55]. A schematic illustration of such a network is shown in figure 21. Alice now plays the role of broadcaster–gatherer and there are now N Bobs, labelled Bob(1) to Bob(N), who can receive downstream signals from Alice and send messages in the upstream direction. The network configuration that we have sketched in figure 21 is known as a 'double star' and it has two layers of optical splitters. A classical multiphoton signal from Alice will be split at these points and a copy of the signal will travel along each emergent path. Eventually each Bob will receive a copy of the original signal transmitted by Alice. Single photons, as we have seen, behave in a very different way at optical splitters.

A single photon sent by Alice cannot be split or copied so that at each splitting layer it will be found in one, and one only, of the possible outputs. The consequence of this is that any single photon input by Alice at the head end will be received by one, *and one only*, of the Bobs. Which Bob receives any given single photon is purely a matter of probability. Thus, in order to establish secret and individual keys with each of the Bobs, Alice sends a randomly coded sequence of single photons as before for the point-to-point quantum key distribution scheme. Each photon in this initial sequence percolates through the network and reaches one of the Bobs. Which Bob receives a given photon is indeterministic and the sequence of time slots for which a given Bob receives a photon will differ for each separate key transmission by Alice. Therefore, a random and unique subset of Alice's tranmission is received by each Bob. This procedure is equivalent to setting up N distinct point-to-point quantum cryptography links between Alice and each of the Bobs. On average, therefore, assuming equal splitting ratios at each layer, each Bob receives a binary string of length D/N where D is the length of Alice's initial transmission. This procedure is sketched in figure 22 for a simplified network consisting of only one splitting layer and three Bobs. It is worth noting that any of the quantum key distribution protocols, including the correlated particle EPR protocol, can be implemented on

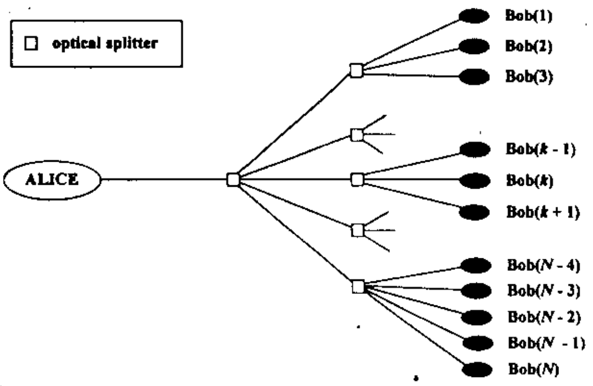


Figure 21. Schematic illustration of a tree-connected network in a 'double star' configuration. Each network node, represented by a square, is an optical splitter. Alice plays the role of broadcaster–gatherer and there are N users on this network.

this optical network. Techniques for using quantum cryptography on other network configurations have been discussed elsewhere [55, 56].

5.2. *Quantum computing and public key systems*

It is an intriguing possibility that quantum mechanics, in the shape of quantum cryptography, will have a significant impact on the security of our future networks. However, if recent ideas prove practicable, quantum mechanics could have a far more serious impact on security provision. In an (as yet), unpublished manuscript Shor [23] of AT&T Laboratories has shown how quantum mechanics can be used to attack some of the most popular cipher systems in use today. In essence, he provided an algorithm to perform a mathematical operation that will run on a quantum computer. The interest lies not in the operation itself, which can be run on a classical computer, but in the speed of the operation which can be many orders of magnitude faster on a quantum machine. In order to see why this invention has caused such a stir we shall have to re-examine some of the ideas that we developed in section 1.

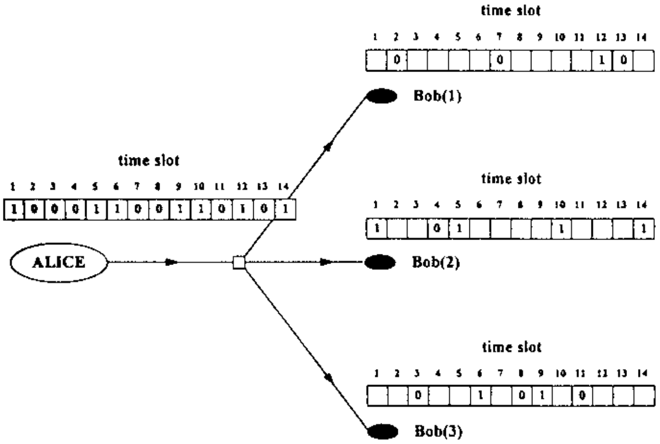


Figure 22. An example of a key transmission on a simplified version of figure 21 with just three network users. We see that each user receives a unique set of single photons and hence a unique bit string.

The kinds of conventional cipher systems that we have so far examined rely on Alice and Bob having either the same secret key, or different secret keys that are easily derived from each other. For this reason such systems are known as symmetric cipher systems. A principal difficulty with these kinds of systems is, of course, that of key distribution. In 1976, Diffie and Hellman developed a new kind of cryptography known as public-key cryptography. In cipher systems of this kind, every user has two keys: a public key and a private key known only to them. Suppose that Alice wished to send a secret message to Bob using a public key cipher system. She would obtain Bob's public key, which could be published in a directory, and use it, together with a public key algorithm, to encrypt her message. The algorithm is such that it is easy to recover the message from the ciphertext with the private key but extremely difficult to do so with only the public key. The public and private keys are in fact related and the public key is generated from the private key quite easily. The reverse process, deriving the private key from the public, however, is extraordinarily difficult. A simple example of mathematical functions which possess this asymmetry is multiplication and division. It is easy to see that the prime numbers 83 and 127 multiplied together give 10 541. The converse is not true; given the number 10 541 it is not an entirely trivial task to determine its factors. As the prime factors become larger, this task becomes almost impossible and even the best factoring algorithms can take months, or even years, on a powerful computer to determine the prime factors of a large number. It is on this difficulty of factorization (and other similarly asymmetric mathematical operations) that the security of a public key system rests.

Although mathematicians have not been able to prove that factorization is a difficult problem,† there is a strong suspicion that it is. However, these assumptions of difficulty have been based on the capabilities of a *classical* computing machine, that is a computer obeying the laws of classical physics. Classical physics is only a subset of quantum mechanics and, if the definition of a computer is enlarged to include machines that can exploit the extra features of quantum mechanics, certain calculations can, in principle, be performed much much faster on a quantum machine. Deutsch [22] laid the foundations for this in 1985 when he generalized

† 'Difficult' in this context relates to the amount of time, or number of logical operations, that it would take a computer to solve the problem. Certain problems, for example, have been shown to require an exponential amount of time to solve in the sense that the solution time goes as exp n, say, where n is the size of the input.

the concept of a Turing machine to include the physical operations allowed by quantum mechanics. This was an important step forward and showed that mathematical models of computation, such as that of a Turing machine, do depend on the specific physics under which such a device is assumed to operate. It was not until very recently, however, that Shor [23] explicitly derived an algorithm for a quantum computer, consistent with the general quantum computational rules of Deutsch, that could perform the operation of factorization many orders of magnitude more quickly than the equivalent calculation on a classical machine. Problems that mathematicians had previously thought to be very difficult to solve could, in principle, be solved in seconds by a quantum computer.

The security of public key cipher systems depends on the supposed difficulty of certain mathematical operations. Shor has shown that at least some of these operations are no longer difficult when performed on a quantum computer. Although still many years away, quantum computers have sounded the death knell for public key cipher systems. Surprisingly, perhaps, quantum key distribution systems are *invulnerable* to this threat from quantum computers. Even a quantum computer cannot beat the uncertainty principle. It is our guess that, as technology edges nearer the capability of building a quantum computer, we shall see the re-emergence of symmetric cipher systems supported by the invulnerability of quantum key distribution.

5.3. *The future?: final remarks*

It is difficult to overemphasize just how radical a departure from classical techniques quantum cryptography is. With quantum cryptography we see the potential of quantum mechanics to lead to fundamentally new techniques in information processing. A classical device simply cannot achieve the functional capabilities of a quantum key distribution system. In quantum computing the case is more evident; the whole theoretical framework of classical computing machines, as developed by Turing, is based upon assumptions of classical mechanics. The laws of classical mechanics have been superseded by the more complete structure of quantum mechanics. In these terms it is not altogether surprising that classical notions of information processing have had to be revised.

From its beginnings in the visionary work of Wiesner, quantum cryptography has progressed from concept to laboratory demonstrator. We hope that we have conveyed in this article some of the excitement of this journey. Quantum cryptography is a multidisciplinary field and we have touched on many aspects of communications technology, cryptography and basic physics. Bennett and Brassard's extension of Wiesner's work to key distribution and the developments in quantum computing have triggered an explosion of effort worldwide. The next few years will undoubtedly see major advances in these areas. It has been our aim in this article to give an account of the current state-of-the-art developments in quantum cryptography from the broad theoretical canvas to the detail of the experimental implementation. We hope we have also given you a glimmer of what the future might have in store for us.

The synthesis of quantum mechanics and information processing has heralded a new era in secure communications. The twin technologies of quantum computing and cryptography present us with both threat and opportunity. In the case of quantum computing those opportunities and threats are almost certainly many years away; quantum cryptography, at least as a laboratory demonstrator, is already here. The successful demonstration of this technique in the laboratory has given fresh impetus to efforts in quantum processing. We are only just beginning to be aware of the potential of quantum systems for processing information in a radically different way. The future is quantum and tomorrow's information technologists will have to be conversant with quantum mechanics to stay ahead of the field.

Acknowledgements

We would like to thank our colleagues Steve Barnett, Keith Blow, Rodney Loudon, John Rarity and Paul Tapster without whom much of this work would have been impossible. We are also indebted to Gilles Brassard for many illuminating and stimulating discussions over the past few years and to Mark Stirland for his continued support.

References

[1] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J., 1992, *J. Cryptol.*, **5**, 3–28.

[2] Wiesner, S., 1983, *Sigact News*, **15**, 78–88 (1983) (original manuscript written about 1970).

[3] Townsend, P. D., Rarity, J. G., and Tapster, P. R., 1993, *Electron. Lett.*, **29**, 634–635.
Townsend, P. D., Rarity, J. G., and Tapster, P. R., 1993, *Electron. Lett.*, **29**, 1292–1293.
Townsend, P. D., and Thompson, I., 1994, *J. Mod. Optics*, **41**, 2425–2434.

[4] Muller, A., Breguet, J., and Gisin, N., 1993, *Europhys. Lett.*, **23**, 383–388.

[5] Townsend, P. D., 1994, *Electron. Lett.*, **30**, 809–810.

[6] Marand, C., and Townsend, P. D., 1995, *Optics Lett.* (submitted).

[7] Marand, C., and Townsend, P. D., 1995, *Electron. Lett.* (submitted).

[8] Franson, J. D., and Ilves, H., 1994, *Appl. Optics*, **33**, 2949–2954.
Franson, J. D., and Ilves, H., 1994, *J. Mod. Optics*, **41**, 2391–2396.

[9] Hughes, R. J., 1995, Private communication; 1995, *Contemp. Phys.*, **36**, 149–163.

[10] Shannon, C. E., 1949, *Bell Syst. Tech. J.*, **28**, 656–715.

[11] Beker, J., and Piper, F., 1982, *Cipher Systems: the Protection of Communications* (London: Northwood Publications).
Brassard, G., 1988, *Modern Cryptology, Lecture Notes in Computer Science*, edited by G. Goos and J. Hartmanis (Berlin: Springer).

[12] Vernam, G. S., 1926, *J. Amer. Inst. Electr. Engrs*, **45**, 109–115.

[13] Chambers, W. G., 1985, *Basics of Communications and Coding* (Oxford: Clarendon), chapter 9, pp. 207–210.

[14] Denning, D. E. R., 1982, *Cryptography and Data Security* (Reading, Massachusetts: Addison-Wesley).

15] Erdmann, E. D., 1992, M.Sc. Thesis, University of London.

16] Diffie, W., and Hellman, M. E., 1976, *IEEE Trans. Inf. Theory*, **IT-22**, 644–654.

17] Bennett, C. H., and Brassard, G., 1984, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 1984 (New York: IEEE), pp. 175–179.

18] Bennett, C. H., Brassard, G., Breidbart, S., and Wiesner, S., 1982, *Advances in Cryptology: Proceedings of Crypto 82* (New York: Plenum), pp. 267–275.

19] Drummond, P. D., and Caves, C. M., 1992, *Quantum Measurements in Optics*, edited by P. Tombesi and D. F. Walls (New York: Plenum), pp. 279–294.

20] 1987, *J. Mod. Optics*, **34**, Nos. 6–7.

21] 1994, *J. Mod. Optics*, **41**, No. 12.

22] Deutsch, D., 1985, *Proc. R. Soc.* A, **400**, 97–117.

23] Shor, P., 1994, in Proceedings 35th Annual Symposium on Foundations of Computer Science (IEEE Computer Society Press), pp. 124–134.

24] Feynman, R. P., Leighton, R. B., and Sands, M., 1964, *The Feynman Lecures on Physics*, Vol. 3 (Reading, Massachusetts: Addison-Wesley).

25] Sakurai, J. J., 1985, *Modern Quantum Mechanics* (Reading, Massachusetts: Addison-Wesley).

26] Blow, K. J., and Phoenix, S. J. D., 1993, *J. Mod. Optics*, **40**, 33–36.

27] Wootters, W. K., and Zurek, W. H., 1982, *Nature*, **299**, 802–803.

28] Phoenix, S. J. D., 1993, *Phys. Rev.* A, **48**, 96–102.

29] Bennett, C. H., Brassard, G., and Robert, J.-M., 1988, *SIAM J. Comput.*, **17**, 210–229.

30] Lütkenhaus, N., 1995, *Phys. Rev.* A (submitted).

31] Bennett, C. H., Brassard, G., Crepeau, C., and Maurer, U. M., 1995, *IEEE Trans. Inf. Theory* (to be published).

32] Wegman, M. N., and Carter, J. L., 1981, *J. Comput. Syst. Sci.*, **22**, 265–279.

33] Bennett, C. H., 1992, *Phys. Rev. Lett.*, **68**, 3121–3124.

34] Loudon, R., 1983, *The Quantum Theory of Light*, second edition (Oxford University Press).

[35] Townsend, P. D., and Poustie, A. J., 1995, *Optics Lett.*, **20**, 37–39.

[36] Owens, P. C. M., Rarity, J. G., Tapster, P. R., Knight, D., and Townsend, P. D., 1994, *Appl. Optics*, **33**, 6895–6901.

[37] Lacaita, A., Cova, S., Zappa, F., and Francese, P. A., 1993, *Optics Lett.*, **18**, 75–77.

[38] Zappa, F., Lacaita, A., Cova, S., and Webb, P., 1994, *Optics Lett.*, **19**, 846–848.

[39] Stenholm, S., 1992, *Ann. Phys. (N.Y.)*, **218**, 233–254.

[40] Ekert, A. K., 1991, *Phys. Rev. Lett.*, **67**, 661–663.

[41] Barnett, S. M., and Phoenix, S. J. D., 1993, *Phys. Rev.* A, **48**, R5–R8.

[42] Cover, T. M., and Thomas, J. A., 1991, *Elements of Information Theory* (New York: Wiley).

[43] Barnett, S. M., and Phoenix, S. J. D., 1991, *Phys. Rev.* A, **44**, 535–545.

[44] Barnett, S. M., Huttner, B., and Phoenix, S. J. D., 1993, *J. Mod. Optics*, **40**, 2501–2513.

[45] Marand, C., and Towsend, P. D., 1995, Unpublished.

[46] Bell, J. S., 1987, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge: Cambridge University Press).

[47] Einstein, A., Podolsky, B., and Rosen, N., 1935, *Phys. Rev.*, **47**, 777–780.

[48] Bell, J. S., 1964, *Physics*, **1**, 195–200.

[49] Franson, J. D., 1989, *Phys. Rev. Lett.*, **62**, 2205–2208.

[50] Ekert, A. K., Rarity, J. G., Tapster, P. R., and Palma, G. M., 1992, *Phys. Rev. Lett.*, **69**, 1293–1295.

[51] Rarity, J. G., and Tapster, P. R., 1992, *Phys. Rev.* A, **45**, 2052–2056. Rarity, J. G., Burnett, J., Tapster, P. R., and Paschotta, R., 1993, *Europhys. Lett.*, **22**, 95–100.

[52] Bennett, C. H., Brassard, G., and Mermin, N. D., 1992, *Phys. Rev. Lett.*, **68**, 557–559.

[53] Barnett, S. M., and Phoenix, S. J. D., 1993, *J. Mod. Optics*, **40**, 1443–1448.

[54] D'Espagnat, B., November 1979, *Sci. Amer.*, 128–140.

[55] Townsend, P. D., Phoenix, S. J. D., Blow, K. J., and Barnett, S. M., 1994, *Electron. Lett.*, **30**, 1875–1877.

[55] Phoenix, S. J. D., Barnett, S. M., Townsend, P. D., and Blow, K. J., 1995, *J. Mod. Optics* (to be published).

imon J. D. Phoenix obtained his B.Sc. in Theoretical Physics from the University of York in 1986 and joined the quantum processing group at BT Laboratories in September 1989 having completed his Ph.D. in Theoretical Quantum Optics under the supervision of Professor P. L. Knight at Imperial College, London. His research interests are focused on the application of novel quantum phenomena to telecommunications.

Paul D. Towsend obtained the degrees of B.Sc. in physics from the University of East Anglia in 1983 and Ph.D. from the University of Cambridge in 1987. He gained post-doctoral experience at Cambridge and Bellcore working on novel photoexcitation and charge transport mechanisms in polymeric semiconductors. Since joining BT in 1990 he has worked on the quantum properties of light and the potential application of these properties to optical communications.

PHYSICAL REVIEW A VOLUME 48, NUMBER 1 JULY 1

Quantum cryptography without conjugate coding

Simon J. D. Phoenix
BT Research Laboratories, Martlesham Heath, Ipswich IP5 7RE, United Kingdom

(Received 16 July 1992)

We extend the quantum key distribution method of Bennett and Brassard [IBM Tech. Discl. Bull. **28**, 3153 (1985)] by exploiting a nonconjugate coding scheme. Using this scheme we are able to show that the original method of Bennett and Brassard gives optimal security.

PACS number(s): 03.65.Bz, 42.79.−e, 89.70.+c

I. INTRODUCTION

One of the most intriguing and exciting recent developments in quantum mechanics has been the prediction and demonstration of a cryptographic key distribution scheme, the security of which is guaranteed by the laws of physics, or, rather, the laws of quantum mechanics [1–3]. The security of these schemes is dependent on the uncertainty principle at a single-particle level. In an ingenious extension to these ideas, Ekert has shown how a quantum-correlated communication channel can be exploited to provide both secure key distribution and secure key storage [4]. The degree of security for the key distribution has been shown to be equivalent for both the Bennett-Brassard and Ekert schemes [5]. What has not, to my knowledge, been demonstrated is that the use of the conjugate coding technique of Wiesner [6] affords *optimal* security for the distribution of the key. One of the aims of the present work is to show that this is indeed the case.

We shall begin by defining the basic notions of quantum alphabets and channels. We shall introduce a measure of conjugacy for alphabets based on the information rate of a quantum channel [7] and relate this to the ability to distribute the key in a secure fashion. By considering an appropriate generalization of the Bennett-Brassard scheme [1,3] to nonconjugate coding we shall show that conjugate coding does indeed provide optimal security. We shall consider only those schemes for which the alphabet symbols are orthogonal although the alphabets are not mutually conjugate. A cryptography scheme can be developed [8] for which the alphabet symbols are not orthogonal, but the alphabets themselves are conjugate. This latter scheme is related to the recent work of Bennett [9]. We shall also discuss briefly ways in which the effectiveness of the Breidbart basis for eavesdropping [1] can be reduced.

II. QUANTUM ALPHABETS

A quantum communication channel is one for which the channel transition probabilities are, in the absence of noise, solely governed by the rules of quantum mechanics. The channel is represented by a set of Hermitian operators which describe the physical properties of the channel. Simple examples of quantum channels are the free-space transmission of single particles such as electrons or photons. What makes these channels truly quantum mechanical is the possibility that the transmission and reception may occur using different alphabets and that the transition probabilities for these alphabets are *entirely determined by the laws of quantum mechanics.* It is the features that quantum mechanics introduces which make such channels particularly interesting. We can think of the Hermitian operators which describe the channel as being the generators of a set of eigenstates which can be used as the symbols of an alphabet. The alphabets need not necessarily contain *all* the eigenstates of a particular operator as its symbols, nor, indeed, do they need to contain symbols generated by only one operator. However, as we shall see, the effectiveness of the alphabet is reduced unless *all* the symbols associated with a *unique* operator are employed.

In order to make some of these notions more precise we shall concentrate on a communication channel between two legitimate users who we shall call "Alice" and "Bob." Alice will transmit messages to Bob using a particular alphabet and Bob will attempt to read the message in his own alphabet. The mutual dependence of the transmitted and received alphabets determines the information transmission rate of the channel. Initially we shall suppose that both Alice and Bob are using alphabets generated from a complete set of eigenstates of the Hermitian operators $\hat{A}$ and $\hat{B}$, respectively. The eigenvalue relations for these operators are

$$\hat{A}|\alpha_j\rangle=\alpha_j|\alpha_j\rangle\ ,\quad \hat{B}|\beta_k\rangle=\beta_k|\beta_k\rangle \qquad (2.1)$$

so that we adopt the terminology that Alice uses the alphabet $\{|\alpha\rangle\}$ sourced by the operator $\hat{A}$ with a similar terminology employed for Bob. We shall make the simplifying, but not restrictive, assumption that the alphabets used by Alice and Bob each have N symbols. This situation is shown schematically in Fig. 1. In general, $\hat{A}$ and $\hat{B}$ are different operators so that Alice and Bob transmit and receive in different alphabets. The channel transition probabilities, in the absence of noise, are determined by the expansion coefficients of the symbols of one alphabet in terms of the other. Thus for the channel that we have just described we find that the probability that Bob receives the symbol $|\beta_k\rangle$ *given* that Alice transmitted the symbol $|\alpha_j\rangle$ is just

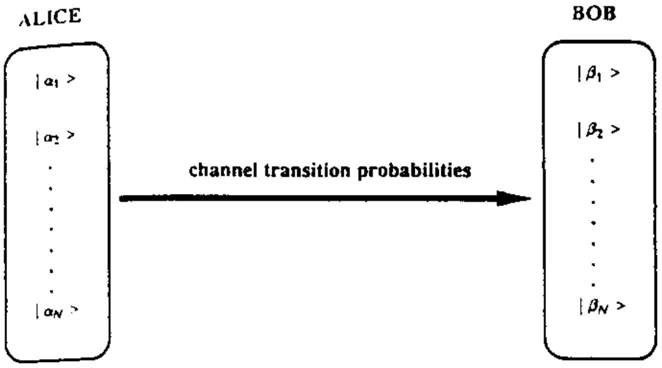


FIG. 1. Schematic illustration of a quantum communication channel in which Alice transmits data using a quantum alphabet $|\{\alpha\}\rangle$ and Bob receives using the quantum alphabet $|\{\beta\}\rangle$. Alice and Bob's alphabets need not necessarily be the same.

$$P(\beta_k|\alpha_j)=|\langle\alpha_j|\beta_k\rangle|^2 , \tag{2.2}$$

where we have employed an obvious, albeit not strictly rigorous, notation. If we now assume that Alice chooses the symbols of her alphabet with equal *a priori* probabilities so that

$$P(\alpha_j)=\frac{1}{N} , \tag{2.3}$$

then the system mutual information, denoted by $J(\hat{A},\hat{B})$, is just given by [7]

$$J(\hat{A},\hat{B})=\ln N+\frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N}|\langle\alpha_j|\beta_k\rangle|^2\ln|\langle\alpha_j|\beta_k\rangle|^2 . \tag{2.4}$$

This quantity is just the mutual information per transmitted and received symbol averaged over both the input and output alphabets. Maximizing $J(\hat{A},\hat{B})$ over the input alphabet gives the channel capacity, which in this case is just $\ln N$. It should be noted that this is also the channel capacity for a perfect classical channel with finite input and output alphabets of equal size.

We now introduce an information-theoretic definition of operator conjugacy. Two operators $\hat{A}$ and $\hat{B}$ are said to be conjugate if their system mutual information is precisely zero. From (2.4) this implies that each input symbol is equally likely to cause any output symbol and we have

$$|\langle\alpha_j|\beta_k\rangle|^2=\frac{1}{N} . \tag{2.5}$$

We have arrived at Wiesner's definition of conjugate variables [6] from the perspective of information theory. This tells us that Alice and Bob can exchange no information on their channel if the alphabets they use are sourced by conjugate operators. In such cases we shall simply describe the alphabets as being conjugate to one another. The difference between the mutual information when both Alice and Bob use the same alphabets and the mutual information when different alphabets are used is the amount of information *lost* when different transmission and reception alphabets are employed. For the simple example we have discussed above, this average lost information is given by

$$\ln N-J(\hat{A},\hat{B})=-\frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N}|\langle\alpha_j|\beta_k\rangle|^2\ln|\langle\alpha_j|\beta_k\rangle|^2 . \tag{2.6}$$

Thus N bits of information (in suitable units) are lost if the communication channel is sourced at input and output by conjugate operators. We can define a dimensionless quantity Q which gives the fraction of information lost by measurement of different alphabets at the input and output of the channel by writing

$$Q=1-\frac{J(\hat{A},\hat{B})}{J(\hat{A},\hat{A})}=1-\frac{J(\hat{A},\hat{B})}{J(\hat{B},\hat{B})} . \tag{2.7}$$

Q varies between 0 and 1 and is zero only when the same alphabets are measured at the input and output, that is, no information is lost. If the input and output alphabets are conjugate, then $Q=1$ and *all* of the information is lost. We can express this in another way. Let us suppose that Alice transmits the symbol $|\alpha_j\rangle$ and that Bob measures the conjugate operator $\hat{B}$. After the measurement, Bob *cannot* reconstruct the information about $\hat{A}$ contained in the original state. It is this irreversible loss of information about the conjugate variable upon measurement which enables the quantum key distribution scheme to work.

Suppose now that Alice and Bob are to try and use their conjugate alphabets to distribute a key for use in a cryptographic application. The protocol can be summarized as follows. Alice and Bob decide to use alphabets sourced by the operators $\hat{A}$ and $\hat{B}$. Alice and Bob are free to choose which of these alphabets to use. They map each of the conjugate alphabets onto a new alphabet of N symbols $1,2,\ldots,N$ so that if Alice transmits $|\alpha_j\rangle$ and Bob measures $\hat{A}$ then Bob reads the symbol "j"; if Alice transmits $|\beta_j\rangle$, which is also equivalent to the symbol j, then Bob has to measure $\hat{B}$ in order to be certain of reading the symbol j from Alice's transmission. Alice and Bob transmit and receive, respectively, by randomly choosing between the two alphabets. Alice and Bob will now have a string of symbols such as $1,3,16,N-4,25,7,N-12,\ldots,$ which will almost certainly disagree. Alice chooses a small subset of these data and asks Bob to discard all of those symbols for which a different choice of alphabet was made. Alice and Bob should now have a set of symbols which are in perfect agreement (in the absence of noise). Any attempt at eavesdropping will disturb this perfect agreement. This comes about because an eavesdropper, Eve, also needs to make a choice between the alphabets. There will be some symbols for which Alice and Eve have used conjugate alphabets, but for which Alice and Bob have used the same alphabet. Eve's intervention will randomize the information encoded in the correct alphabet and so lead to the possibility that Alice and Bob will obtain a different result even though they have used the same alphabet. Alice and Bob will be able to determine whether or not an attempt at interception has been made.

Let us formalize the above discussion. Suppose that Alice transmits the symbol j as the state $|\alpha_j\rangle$. In the absence of any interception, Alice and Bob will only agree to use this information *if and only if* both Alice and Bob use the same alphabets. In this case, for example, Bob will have chosen to orient his detection apparatus to measure the operator $\hat{A}$ and will, with unit probability, have measured the symbol j. The situation is different in the presence of an eavesdropper. Suppose that the eavesdropper, Eve, chooses to measure $\hat{A}$. In this case Eve will read the symbol j with unit probability. Shen then transmits the state $|\alpha_j\rangle$ to Bob who can decide to measure either of the conjugate alphabets. It is important to keep in mind the fact that Alice and Bob will simply discard those results for which different choices of input and output alphabets were used. If Eve chooses to measure $\hat{B}$ then she will read the symbol j with probability $1/N$. Eve has no sensible option other than to retransmit faithfully to Bob the state she thinks she has observed. This is because Eve has no way of knowing whether her choice of measurement was, in fact, correct. Eve then, after measurement of $\hat{B}$, will retransmit some state $|\beta_k\rangle$. Upon reception of this state, Bob, choosing to make a measurement of $\hat{A}$, will read the symbol j with probability $1/N$. Alice and Bob upon subsequent communication will find, with probability $(N-1)/N$, that they do not agree about this result. Clearly, for a perfect channel in the absence of eavesdropping Alice and Bob *must* agree about every result for which they make the same choice of alphabets. Overall then, per transmission, the probability that Eve will escape detection is given by

$$P_{\text{esc}}=\frac{1}{2}\left[1+\frac{1}{N}\right] . \tag{2.8}$$

If Alice and Bob compare M results then the probability that Eve will escape detection is just $(P_{\text{esc}})^M$. If N, the alphabet size, is quite large then Eve's chances of escaping detection are approximately 2^{-M}, which rapidly becomes negligible as M is increased. Current experimental and theoretical key distribution schemes use an alphabet size of $N=2$ [1,4,10]. In the next sections we shall restrict ourselves to this dimensionality, noting, however, that the dimensionality of the alphabet space can be increased.

III. KEY DISTRIBUTION WITHOUT CONJUGATE CODING

The essential ingredient of a conjugate coding scheme is that measurement of the incorrect variable will give precisely no information about its conjugate. However, one can envisage situations in which a measurement of the incorrect variable will give *partial* information about the other, correct, variable. We show in this section that a secure key distribution scheme can still be implemented in this case although a longer subset of data is needed to achieve a given degree of security. We shall consider an alphabet size of 2 and shall consider the standard spin variables as the operators which generate our alphabets. We shall consider a spin variable aligned along the z direction and a spin variable aligned at angles θ and ϕ to

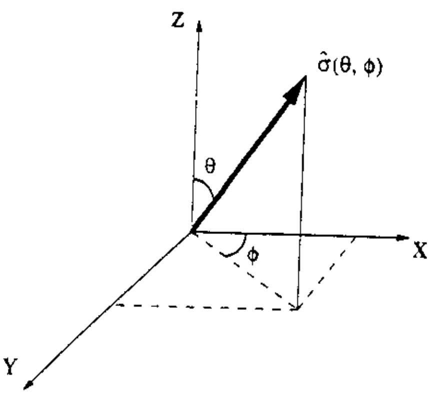


FIG. 2. Geometric representation of the spin variables which are characterized by the angles θ and ϕ.

this. This is shown schematically in Fig. 2. We label the spin operators in these directions by $\hat{\sigma}_z$ and $\hat{\sigma}(\theta,\phi)$. The non-Hermitian spin-flip operators associated with the direction of spin are labeled by $\hat{\sigma}_{\pm}$. The eigenstates of the spin-z operator can be expanded in terms of the eigenstates of $\hat{\sigma}(\theta,\phi)$ and vice versa so that we have the expansions

$$\begin{aligned}|+\rangle_{\theta,\phi}&=\cos(\theta/2)\exp(-i\phi/2)|+\rangle_z\\&\quad+\sin(\theta/2)\exp(i\phi/2)|-\rangle_z ,\\|-\rangle_{\theta,\phi}&=-\sin(\theta/2)(-i\phi/2)|+\rangle_z\\&\quad+\cos(\theta/2)\exp(i\phi/2)|-\rangle_z ,\end{aligned} \tag{3.1}$$

and the complementary expansions

$$\begin{aligned}|+\rangle_z&=\exp(i\phi/2)[\cos(\theta/2)|+\rangle_{\theta,\phi}\\&\qquad-\sin(\theta/2)|-\rangle_{\theta,\phi}] ,\\|-\rangle_z&=\exp(-i\phi/2)[\sin(\theta/2)|+\rangle_{\theta,\phi}\\&\qquad+\cos(\theta/2)|-\rangle_{\theta,\phi}] .\end{aligned} \tag{3.2}$$

Although it is not necessary to do so at this stage we have retained the phase factors in these expressions as these are important when we consider an attack using the Breidbart basis [1].

Let us suppose that Alice and Bob wish to set up a secure key distribution scheme using the two alphabets generated by these spin operators. The alphabets consist of the z states $\{|\pm\rangle_z\}$ and the θ-states $\{|\pm\rangle_{\theta,\phi}\}$. Alice sends to Bob a random sequence of the symbols "1" and "0" by randomly choosing between the states of these alphabets. Alice and Bob will have previously agreed to read a spin-up result as a logical 1 and a spin-down result as a logical 0. In the *absence* of interception, the probability that Bob will read the symbol that Alice actually sent is just

$$P(\text{Bob correct: no interception})=1-\tfrac{1}{2}\sin^2(\theta/2) . \tag{3.3}$$

After Alice and Bob have discarded those bits for which they used different alphabets this probability rises to unity. Physically there can be no difference between an eavesdropper and the legitimate receiver. Consequently the above probability (3.3) is also the probability that Eve will read the correct symbol. However, *after* interception Eve and Bob are no longer indistinguishable as far as the channel is concerned. This is because Eve has disturbed the information encoded in some of the spins sent by Alice. Eve must retransmit the spin in order to try and fool Alice and Bob and, in this case, the probability per bit that Bob and Alice agree, after discarding the appropriate bits, is no longer unity but is given by

$$P(\text{Bob correct: after Eve's retransmission}) = 1-\tfrac{1}{4}\sin^2\theta \ . \qquad (3.4)$$

This is also clearly equal to the probability, per bit, that Eve escapes detection after an attempt at interception of the key. The key distribution schemes currently in the literature [1,3,4] all employ conjugate coding which for the spin operators discussed above are equivalent to the choice $\theta=\pi/2$. In this case we have that the probability that Eve escapes detection per bit is $\frac{3}{4}$. Suppose now that Alice and Bob need to compare K bits of data for a *conjugate* coding scheme in order to achieve a given degree of certainty that an interception has not taken place. Let M be the number of bits that Alice and Bob have to compare in a *nonconjugate* coding scheme, such as that discussed above, in order to achieve the same degree of certainty as for the conjugate scheme. The ratio of the number of bits M/K is then given by

$$\frac{M}{K}=\frac{\ln(\frac{3}{4})}{\ln[1-\frac{1}{4}\sin^2\theta]} \ . \qquad (3.5)$$

This ratio is plotted in Fig. 3. It should be noted that the penalty for using a nonconjugate scheme does not become prohibitively severe until the angle between the spin operators is about $\pi/3$. The graph demonstrates that secure key distribution is possible for a nonconjugate coding scheme, however the number of bits of data which Alice and Bob need to compare to achieve a given degree of security increases as the degree of conjugacy decreases. The ratio M/K is also equal to the ratio of the information gains per received bit about the eavesdropping attempt for the conjugate and nonconjugate coding schemes.

It is clear from the figure that conjugate alphabets ($\theta=\pi/2$) give the greatest degree of protection against interception for this particular key distribution and this particular eavesdropping attempt. However, there are alternative distribution schemes and different methods of interception. Alice could, for example, use biased statistics in her choice of alphabets, as could Bob. Equally, Eve could use the Breidbart basis which increases her chances of reading the correct bit without compromising her chances of escaping detection [3]. In the following sections we examine these various options open to both the legitimate and illegitimate users of the channel.

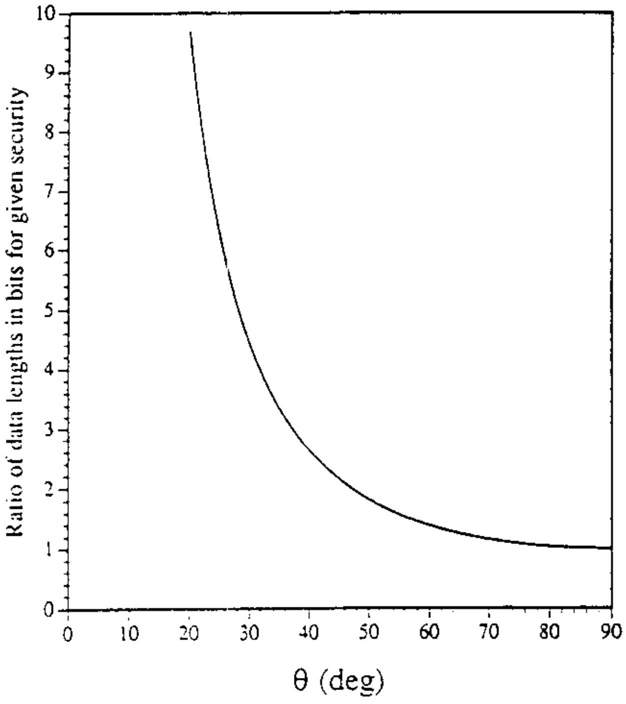


FIG. 3. The ratio of the lengths, in bits, of the data sets for conjugate and nonconjugate coding needed to achieve the same degree of channel security as a function of θ.

IV. THE BREIDBART BASIS AND RANDOM STATISTICS

Eve is clearly not restricted from choosing any particular direction in which to orient her measuring apparatus. It has been shown [3] for the case of unbiased transmission statistics and conjugate alphabets that Eve's optimum strategy is to align her apparatus to measure spin at $\pi/4$ and to retransmit in this basis. Her chances of escaping detection remain at 75% per bit but her chances of reading the bit correctly increase to nearly 85% [3]. This basis is known as the Breidbart basis. We shall continue to use this terminology for the basis which "bisects" the alphabets, even though this may not prove to be the optimum strategy for Eve. What should Eve do to optimize her chances if nonconjugate coding is employed and one of the alphabets is, for example, only chosen 40% of the time, on average? Let us first examine Eve's measurement basis or alphabet. We shall assume that Eve aligns her apparatus at the angles θ' and ϕ' with respect to the z direction of spin (refer to Fig. 2). We shall write $\psi=\phi-\phi'$ to denote the phase difference between Eve's alphabet and the θ alphabet used by Alice and Bob. We should note that Eve merely orients her apparatus to measure the Breidbart alphabet and does not have to make a choice between alphabets. This is slightly different to her strategy if she uses the legitimate alphabets. The expansion equivalent to (3.1) and (3.2) are achieved for Eve's basis by the simple expedient of replacing unprimed quantities with the respective primed versions. The expansions of the θ alphabet in terms of Eve's alphabet, and vice versa, are easy to obtain by a simple substitution procedure and we find, for example, that the spin-up state in the θ alphabet has an expansion in terms of Eve's alphabet given by

$$|+\rangle_{\theta,\phi}=[\cos(\theta/2)\cos(\theta'/2)\exp(-i\psi/2)+\sin(\theta/2)\sin(\theta'/2)\exp(i\psi/2)]|+\rangle_E$$
$$+[\sin(\theta/2)\cos(\theta'/2)\exp(i\psi/2)-\cos(\theta/2)\sin(\theta'/2)\exp(-i\psi/2)]|-\rangle_E\ ,$$

with similar expressions for the other expansions. We have used the subscript E to denote the eigenstates which form Eve's alphabet.

We shall assume, for the moment, that Alice makes a completely random choice between her available alphabets so that each alphabet is chosen with a probability of $\frac{1}{2}$. Let us further assume that Alice transmits the state $|+\rangle_{\theta,\phi}$. Eve reads the symbol 1 with a probability given by

$$|\cos(\theta/2)\cos(\theta'/2)\exp(-i\psi/2)$$
$$+\sin(\theta/2)\sin(\theta'/2)\exp(i\psi/2)|^2$$

and retransmits the state $|+\rangle_E$ to Bob. If Bob aligns his apparatus to measure in the θ direction then he reads 1 with this probability also. There are two important probabilities to determine. The first is the probability that Eve reads the correct bit and the second is the probability that Eve escapes detection. The probability that Eve reads the correct bit is determined from the expansion coefficients such as those in (4.1) and, after some trigonometric manipulation, we find that

$$P(\text{Eve correct})=\tfrac{1}{2}+\tfrac{1}{4}(1+\cos\theta)\cos\theta'$$
$$+\tfrac{1}{4}\sin\theta\sin\theta'\cos\psi\ . \qquad (4.2)$$

It is an easy task now to determine which angle should measure to maximize her chances of reading correct bit. we find that Eve should choose the a given by

$$\theta'=\tan^{-1}\left[\frac{\sin\theta}{1+\cos\theta}\right]=\theta/2\ . \qquad ($$

This shows that, when Alice uses unbiased statistic choose between the alphabets, the Breidbart basis is basis which gives the maximum chance for the ea dropper to determine the correct bit. However, this tential advantage is of no use to an eavesdropper if use of such a basis increases the chances for the leg mate users of the channel to detect her presence. Guic by previous work [1] which examines the situati $\theta=\pi/2$, we should expect that the use of this basis d not confer any disadvantage on the eavesdropper as far her chances of escaping detection. The probability tl Eve escapes detection is the same as the probability tl Alice and Bob agree after having rejected those resu which were taken for different alphabets. This can al be determined from the eigenstate expansions such (4.1) and we find that, for unbiased choice of alphabet the probability that Eve escapes detection is

$$P(\text{Eve escapes detection})=\tfrac{1}{2}(1-\tfrac{1}{2}\sin^2\theta')(2-\tfrac{1}{2}\sin^2\theta)+\tfrac{1}{8}[2\cos^2\psi+1]\sin^2\theta\sin^2\theta'+\tfrac{1}{2}\cos\theta\cos\theta'\sin\theta\sin\theta'\cos\psi\ . \qquad (4.$$

This, of course, reduces to the expected value of $\frac{3}{4}$ when $\theta=\theta'=\pi/2$, but, more significantly, it reduces to the value $1-\frac{1}{4}\sin^2\theta$ when $\theta=\theta'$, which is our previous result. The question to be answered is whether Eve benefits from use of the Breidbart basis as far as her chances of escaping detection are concerned. For the Breidbart basis we have Eve's choice $\theta'=\theta/2$ and (4.4) reduces to

$$P(\text{Eve escapes detection: Breidbart})=1-\tfrac{1}{2}\sin^2(\theta/2)\ . \qquad (4.5)$$

These results are plotted in Figs. 4(a) and 4(b) in which we plot the graphs of the relevant probabilities for Eve in the cases when she does and does not use the Breidbart basis. It is clear from these graphs that Eve's chances of escaping detection *increase* if she uses the Breidbart basis when Alice and Bob employ a nonconjugate coding scheme. In fact, differentiation of (4.4) with respect to θ' shows that this quantity is *maximized* at $\theta'=\theta/2$. The Breidbart basis is clearly optimal for Eve. For the special case of conjugate coding, $\theta=\pi/2$, Eve's chances of escaping detection remain unchanged.

So far in this section we have considered only an equal random choice between the alphabets. Let us suppos now that Alice chooses to send the z alphabet with probability P_z^A and the θ alphabet with probability P_θ^A such that $P_z^A+P_\theta^A=1$. Let us also suppose that Eve *not* using the Breidbart basis, for the moment. Eve is als free to choose between alphabets and we use the superscript "E" to denote the relative probabilities with which Eve chooses these alphabets. Let us suppose that Alice sends the state $|+\rangle_z$ the probability that Eve reads the correct bit 1 given that Alice transmitted this state is given by

$$P(\text{Eve correct}|\ \text{Alice sends}|+\rangle_z)$$
$$=P_z^E+P_\theta^E\cos^2(\theta/2)\ . \qquad (4.6)$$

Working out these probabilities for all possible transmitted states and combining them gives the probability that Eve reads the correct bit for *any* transmitted state as

$$P(\text{Eve correct})$$
$$=1-[P_\theta^A+P_\theta^E-2P_\theta^A P_\theta^E]\sin^2(\theta/2)\ . \qquad (4.$$

A similar exercise in probability calculus gives the prob bility that Eve escapes detection as

$$P(\text{Eve escapes detection}) = 1-\tfrac{1}{2}[P_\theta^A+P_\theta^E-2P_\theta^A P_\theta^E]\sin^2\theta \ . \quad (4.8)$$

Both of these expressions reduce to $\frac{1}{4}$ for conjugate alphabets and equal *a priori* choice of alphabets. It should be noted that the term in square brackets is common to both expressions and clearly Eve must minimize this quantity to optimize her chances of successful interception using these alphabets. However, the only parameter which is under the direct control of Eve is the relative probability P_θ^E with which she chooses to measure the alphabets. From (4.7) and (4.8) we see that if Alice, in fact, makes an equal *a priori* choice of alphabets so that $P_\theta^A=\frac{1}{2}$, then Eve's choice of alphabet is irrelevant and she could align her apparatus along a single direction. If, on the other hand, Alice chooses $P_\theta^A>\frac{1}{2}$, then Eve minimizes the quantity in square brackets by choosing $P_\theta^E=1$. Conversely, if Alice chooses to transmit more frequently in the z alphabet, then Eve must orient her apparatus to measure along this direction to optimize her chances. Eve's strategy is based on an all or nothing choice, rather than a precise reflection of Alice's transmission statistics as we might have expected at the outset. Alice's best strategy is to remove any control Eve may have over the channel and the only way she can do this is by resorting to an equal *a priori* choice of alphabets so that $P_\theta^A=\frac{1}{2}$.

As a final illustration of the kind of complexities that can occur, let us now suppose that Alice uses biased transmission statistics and that Eve chooses to measure in a single alphabet characterized, as before, by the angles θ' and ϕ'. We shall, for the moment, set the relative phase $\psi=0$. The probability that Eve reads the correct bit is now given by

$$P(\text{Eve correct})=\tfrac{1}{2}(1+\cos\theta') + \frac{P_\theta^A}{2}(\sin\theta\sin\theta'+\cos\theta'[\cos\theta-1]) \ . \quad (4.9)$$

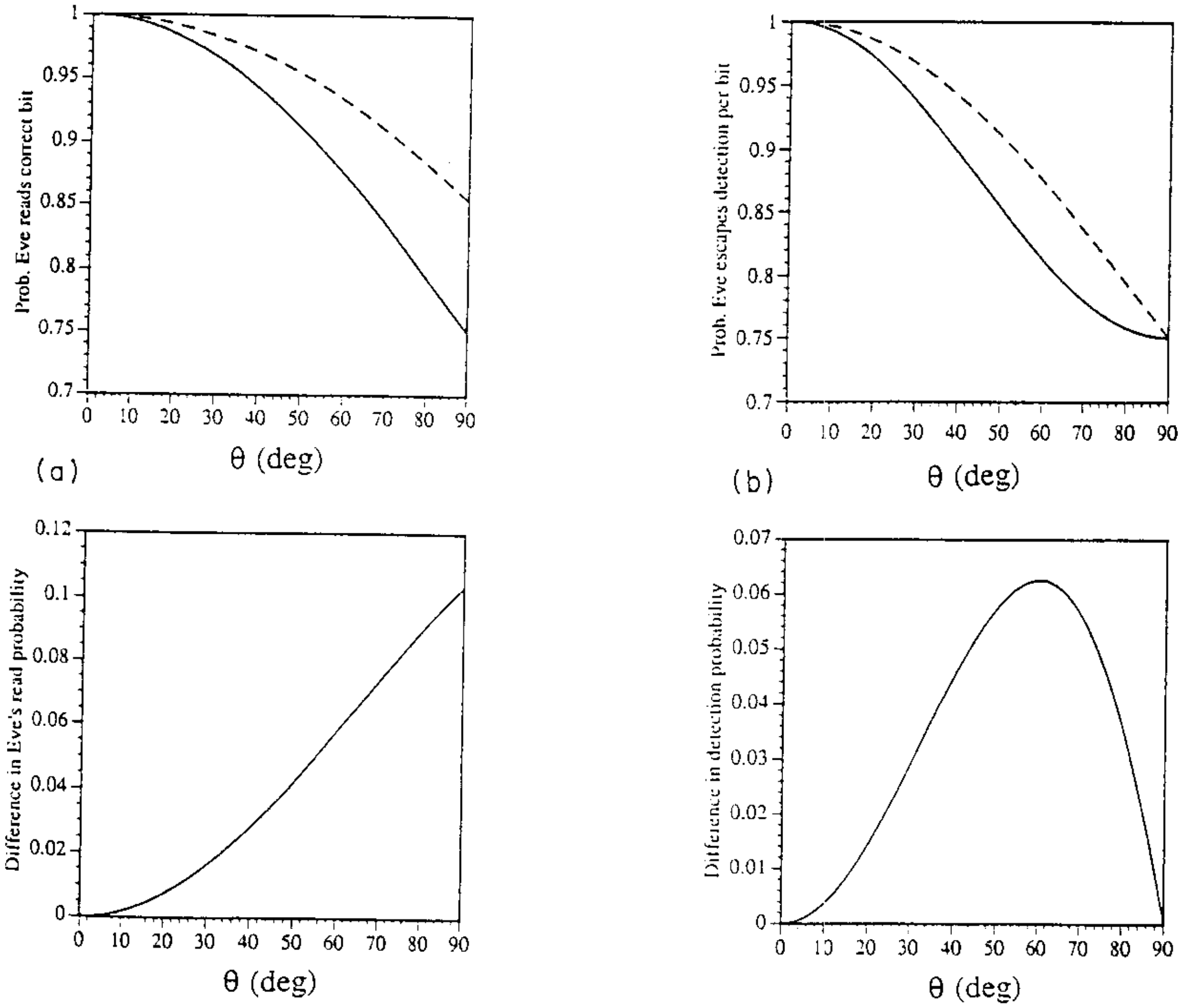


FIG. 4. (a) The probability that Eve reads the correct bit upon interception is plotted as a function of θ. The solid line is for an interception scheme based on the legitimate alphabets, and the dashed line is for an interception using the Breidbart basis. The lower graph gives the difference between these curves as a function of θ. (b) The probability that Eve escapes detection, per bit, as a function of θ. The solid line is for an interception scheme based on the legitimate alphabets, and the dashed line is for an interception using the Breidbart basis. The lower graph gives the difference between these curves as a function of θ.

Maximizing this quantity with respect to θ' shows that the angle Eve must choose is given by

$$\theta' = \tan^{-1}\left[\frac{P_\theta^A \sin\theta}{1-P_\theta^A+P_\theta^A\cos\theta}\right]. \tag{4.10}$$

Only if Alice makes an equal *a priori* choice of alphabet does this angle exactly bisect the alphabets. The effect of Alice's biased transmission statistics is to shift Eve's optimal angle away from the Breidbart angle which bisects the two alphabets. However, the angle given in (4.10) merely maximizes Eve's chances of reading the correct bit if Eve uses some intermediate basis. We also need to determine the probability that Eve remains undetected. This can again be worked out quite simply by following through all the relevant probabilities and for $\psi=0$ we find that the angle Eve must choose to minimize the chance that she will be detected is given by

$$\theta' = \tfrac{1}{2}\tan^{-1}\left[\frac{P_\theta^A \sin 2\theta}{1-P_\theta^A+P_\theta^A\cos 2\theta}\right], \tag{4.11}$$

which is clearly not equal to the angle (4.10) which optimizes Eve's chances of reading the correct bit. These angles coincide, of course, when Alice chooses each alphabet with equal likelihood.

V. DISCUSSION AND CONCLUSIONS

It is easy to see from an information-theoretic viewpoint exactly why a conjugate coding scheme has to be optimal. It is not so easy to see whether a nonconjugate coding scheme can work when the loss of information on measuring the incorrect basis is only partial. We have demonstrated in this article that a nonconjugate coding scheme can, in fact, give a secure key distribution. In doing so we have established the limits of the technique and have explicitly shown that conjugate coding [1] is indeed the optimal strategy for the legitimate users of the channel. Our analysis has been based on the protocol that Alice and Bob will reject any measurement for which they used different alphabets. This is, in fact, unnecessarily restrictive and Alice and Bob can gain statistical information about the eavesdropper if they are prepared to consider some of their rejected data [11]. This reduces the length of data that Alice and Bob will need to collect in order to perform a reasonable statistical test on their results to check for eavesdropping. The lower bound is given by a conjugate coding scheme and the upper bound is given by the protocol described in this paper.

We have examined the use of the Breidbart basis for the eavesdropper and have shown that it is *more* effective if used when a nonconjugate coding scheme is being employed. Thus not only are the legitimate users handicapped by having to collect more data they are also more vulnerable to attack by an eavesdropper employing the Breidbart basis. There is a way, however, to reduce th effectiveness of the Breidbart basis which will reduc Eve's chances of reading the correct bit at the expense o having to collect more data. The essential thing to notic is that there are three mutually conjugate alphabets for . two-dimensional Hilbert space [6]. Alice and Bob ca reduce the effectiveness of the Breidbart basis if Alic uses all three alphabets to transmit data. Eve is at disadvantage in adopting the Breidbart basis as we ca see from (4.2) and (4.4). The important thing to note that the read and detection probabilities for Eve a influenced by the relative phase ψ. Eve cannot but he in disturbing the measurement statistics when using t Breidbart basis when $\psi=\pi/2$. Unfortunately the use of third alphabet which is essentially performing no usef function other than to give statistical information abo an eavesdropper requires the collection of more data Alice and Bob and the use of a slightly different proto [12]. The benefit accrued is small compared to the ex complexity. It should also be noted that even though t use of the Breidbart basis for a conjugate coding sche can give about 85% chance per bit for an eavesdropper determine the correct key this statistical information be reduced by a privacy amplification technique [Furthermore, with a 75% per bit of remaining undet ed Eve's chances of escaping detection for a reason data set are effectively negligible.

ACKNOWLEDGMENTS

I would like to thank G. McLaren of the Secure tems section at BT Labs for many helpful discussions ideas throughout this work. I would also like to thar M. Barnett and K. J. Blow for their suggestions.

[1] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology: Proceedings of Crypto '82* (Plenum, New York, 1983).

[2] C. H. Bennett and G. Brassard, IBM Tech. Discl. Bull. **28**, 3153 (1985).

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Crypt. 5, 3 (1992).

[4] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[6] S. Wiesner, SIGACT News **15**, 78 (1983).

[7] S. M. Barnett, D. T. Pegg, and S. J. D. Phoenix (unpublished).

[8] S. J. D. Phoenix (unpublished).

[9] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[10] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. P Phys. Rev. Lett. **69**, 1293 (1992).

[11] S. M. Barnett and S. J. D. Phoenix, this issue, Phys. A (to be published); K. J. Blow and S. J. D. Phoer Mod. Opt. **40**, 33 (1993).

[12] This protocol and another more sophisticated proto volving four conjugate alphabets, will be discussec where.

[13] C. H. Bennett, G. Brassard, and J-M. Robert, SI Comput. **17**, 210 (1988).

PHYSICAL REVIEW A VOLUME 60, NUMBER 3 SEPTEMBER 1999

Quantum cryptographic device using single-photon phase modulation

Jean-Marc Mérolla,[1] Yuri Mazurenko,[1] Jean-Pierre Goedgebuer,[2] Laurent Duraffourg,[1] Henri Porte,[2] and William T. Rhodes[1]

[1]*GTL-CNRS Telecom, UMR CNRS 6603, Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France*

[2]*Laboratoire d'Optique P. M. Duffieux, UMR 6603, Université de Franche-Comté, 25030 Besançon Cedex, France*

(Received 26 October 1998)

We report a particular implementation of a quantum cryptographic device operating at 1540-nm wavelength and involving interference between phase-modulated sidebands produced by a pair of phase modulators in the transmitting and receiving modules. The principle of operation is described in terms of both classical and quantum optics. The method has been demonstrated experimentally using a strongly attenuated semiconductor laser diode. Single photon interference has been obtained with a fringe visibility greater than 90%, indicating that the system can be used for quantum key distribution. [S1050-2947(99)06608-1]

PACS number(s): 03.67.Hk, 03.67.Dd, 42.79.−e

I. INTRODUCTION

The objective of quantum key distribution is to exploit fundamental properties of quantum optics in order to share in secret a random bit sequence—the key—between two users, Alice and Bob. Once the sharing is carried out, the two parties can exchange a message over a public channel by encrypting with the key a message of equal length. If the key is used only once, the message cannot be deciphered by an eavesdropper, Eve, who does not possess the key [1]. The problem of this one-time-pad method is that the key must be transmitted without any possibility of interception. If the key distribution is effected by nonsecure transmission lines, the key can be detected by an eavesdropper without the knowledge of the legitimate users.

One of the most unexpected developments in quantum optics has been the demonstration of cryptographic key distribution schemes where security is guaranteed by fundamental laws of quantum mechanics [2,3] instead of by mathematical algorithms as in classical cryptographic methods. In quantum key distribution, the key is sent over a quantum channel. If Eve taps the line, transmission errors occur due to the quantum-mechanical nature of photons. To detect these errors, the legitimate users verify statistically a set of shared bits. If too many errors are detected in the verification process, the users discard those bits.

Such a polarization encoding method has been demonstrated in a free-space transmission in anticipation of potential applications to satellite secure communications, and in a transmission on standard optical fibers [4,5]. One of the most spectacular results in terms of systems was the demonstration performed over a 22-km-long fiber submerged in Lake Geneva [6]. Unfortunately, fiber transmission inevitably leads to problems associated with polarization preservation if standard single-mode fibers are used. Thus, in recent years, another quantum-optic method has seen increased interest. In this second method, photons with delay-coded states are used. Encoding and decoding of the bit information are implemented through optical delays introduced by a pair of fiber interferometers characterized by large optical path-length differences (typically 1 m) set in the emitter (Alice) and the receiver (Bob). The receiver can then recognize every bit sent by the sender if the pair of interferometers is closely matched in path length one to each other. However, the existence of a noninterfering signal, decreasing the maximum visibility interference of 50%, requires the use of time-gated detection and polarization division to achieve high visibility (0.99) [7]. Moreover, the interferometers must remain stable in the presence of environmental perturbations, i.e., the path-length differences in the interferometers must be held constant. Feedback loops driving piezoelectric fiber stretchers set in the interferometers have been used to compensate mechanical vibrations and thermal drift. However, despite active compensation, transmissions have been reported to be limited to some few seconds (5 sec for a slow thermal drift that occurs at a rate of 0.6 rad/min), sufficient only to demonstrate the possibility of key distribution over 30 km of standard fiber [7]. An elegant method using Faraday mirrors has been proposed to overcome the effects of polarization fluctuations in the transmission line [8]. Other approaches, based on wavelength or frequency coding, have also been proposed recently [9,10].

We describe here a system that uses single photons with phase-encoded states and operating with a nonorthogonal two-state scheme. Phase-encoded states are produced by an integrated electro-optic phase modulator set in the transmitter, which uses an attenuated semiconductor laser to produce a sequence of countable photons. Since to the best of our knowledge the method is new in the area of optical cryptography, we begin by explaining the principle of operation in a combination of classical and quantum terms. We introduce an appropriate version of a two-state protocol [3] and relate this to the ability to distribute a key in a secure fashion. We also report experimental results obtained at 1540-nm wavelength that show some interesting features of the method, especially its great simplicity.

II. PRINCIPLE OF OPERATION

In the transmission system shown in Fig. 1, the transmitter (Alice) consists of an integrated electro-optic phase modulator PM$_1$ powered by a single-frequency semiconductor laser operating at angular frequency ω_0, referred to subsequently as the reference frequency. The laser output is strongly attenuated by a variable fiber attenuator (this point is discussed in greater detail later, since the attenuation re-

1050-2947/99/60(3)/1899(7)/$15.00

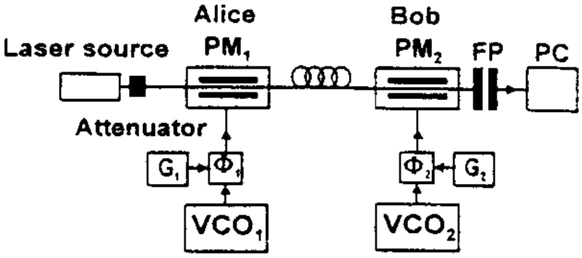


FIG. 1. Schematic diagram of the phase-modulation transmission system.

quired differs from that of previously reported methods). The reference laser beam is phase-modulated by PM_1, which is driven by a voltage-controlled oscillator VCO_1 operating at a fixed frequency Ω but with a phase Φ_1 that can be changed randomly between two states, namely 0 and π for bit "0" and "1," respectively. These two phase states determine the basis used by Alice. A random bit generator G_1 is used by Alice to drive the phase of VCO_1. At the output of Alice's modulator, light is phase-modulated, and sideband frequencies $\omega_0+\Omega$ and $\Omega_0-\Omega$ are induced in the spectrum of light. The phase of those sideband frequencies is Φ_1. The receiver (Bob) consists of a second phase modulator PM_2 driven by a sine voltage provided by a voltage controlled oscillator VCO_2 operating at the same frequency Ω. A random bit generator G_2 switches the phase Φ_2 of that sinusoidal signal randomly between two values 0 and π. These values will be used by Bob to recognize the bits sent by Alice, as will be explained in Sec. III. When phase modulating the light, Bob also generates sidebands in the spectrum, including two with frequencies $\omega_0+\Omega$ and $\omega_0-\Omega$ with phase Φ_2. Depending on the value of Φ_2 relative to Φ_1, constructive or destructive interference can occur between the sidebands generated by Alice and Bob. To analyze such interference, Bob's receiver contains a Fabry-Pérot interferometer FP and a photon counter PC. The FP operates as a spectral filter with its transmission peak adjusted at one side frequency, e.g., $\omega_0+\Omega$. Let us now assume that Alice has sent single photons in a state Φ_1 in the sideband frequency $\omega_0+\Omega$ selected by the FP. The probability that Bob detects the photon at the FP output depends on the value he chooses for Φ_2. Assuming the transmission and the detection are ideal, i.e., lossless and error-free, the probability is 0% as $|\Phi_2-\Phi_1|=\pi$ (Alice's and Bob's modulations out of phase), and 100% as $|\Phi_2-\Phi_1|=0$ (modulations in quadrature). As Bob detects a photon with his phase set on 0 and π, he reads bit "0" and bit "1," respectively. The working conditions yielding such specific properties of the system, as exploited for quantum key distribution, are now explained.

Initially we assume that the laser diode operates as a classical source, not strongly attenuated. Let $E=E_0\exp(j\omega_0 t)$ be the light field associated with angular frequency ω_0 emitted by the laser diode and injected in Alice's modulator. The light obtained at the modulator output can be expressed as

$$E_1(t)=E_0\exp j[\omega_0 t+m_1\sin(\Omega_1 t+\Phi_1)], \tag{1}$$

where $\phi_1(t)=m_1\sin(\Omega_t t+\Phi_t)$ is the phase modulation introduced by Alice's modulator, and m_1, Ω_1, and Φ_1 its amplitude (also termed *modulation depth* in the following), angular frequency, and phase, respectively. This light field is sent to Bob's phase modulator, yielding a light field expressed as

$$E_2(t)=E_1(t)\exp j[m_2\sin(\Omega_2 t+\Phi_2)], \tag{2}$$

where $\phi_2(t)=m_2\sin(\Omega_2 t+\Phi_2)$ is the phase modulation produced by Bob's modulator, with m_2, Ω_2, and Φ_2 its amplitude, angular frequency, and phase, respectively. Setting $\Omega_1=\Omega_2=\Omega$ and $m_1=m_2=m$, we obtain

$$E_2(t)=E_0\exp j[\omega_0 t+A\sin\{\Omega t+(\Phi_1+\Phi_2)/2\}], \tag{3}$$

with $A=2m\cos\{(\Phi_2-\Phi_1)/2\}$. Finally, the light field at the spectral filter output is the spectrum in amplitude of $E_2(t)$. It can be calculated by expressing Eq. (3) as a series of Bessel functions. Recalling that

$$\exp(jA\sin\theta)=\sum_{n=-\infty}^{\infty}J_n(A)\exp(jn\theta)\quad\text{and}$$

$$J_n(-A)=(-1)^n J_n(A),$$

where J_n is the nth-order Bessel function, Eq. (3) can also be written as

$$E_2(t)=\sum_{n=-\infty}^{\infty}J_n[2m\cos\{(\Phi_2-\Phi_1)/2\}]E_0$$
$$\times\exp j[(\omega_0+n\Omega)t+n(\Phi_1+\Phi_2)/2\}]. \tag{4}$$

Assuming the modulation depth m is much smaller than 1 rad, the expression for $E_2(t)$ can be approximated as

$$\begin{aligned}E_2(t)\approx{}&J_0\{2m\cos[(\Phi_2-\Phi_1)/2]\}E_0\exp j(\omega_0 t)\\&-J_1\{2m\cos[(\Phi_2-\Phi_1)/2]\}E_0\exp j[(\omega_0-\Omega)t\\&-(\Phi_1+\Phi_2)/2]+J_1\{2m\cos[(\Phi_2-\Phi_1)/2]\}E_0\\&\times\exp j[(\omega_0+\Omega)t+(\Phi_1+\Phi_2)/2].\end{aligned} \tag{5}$$

The light field $E_2(t)$ at the output of Bob's modulator is formed by a center spectral component at frequency ω_0 and two side components at $\omega_0+\Omega$ and $\omega_0-\Omega$. The Fabry-Pérot selects the $\omega_0+\Omega$ frequency. Assuming again that the modulation depth is small ($m\ll 1$), the intensity in the center band is E_0^2 while Bob detects at his Fabry-Pérot output an intensity expressed as

$$\begin{aligned}i={}&E_0^2J_1^2\{2m\cos[(\Phi_2-\Phi_1)/2]\}\\&\approx 4m^2E_0^2\cos^2[(\Phi_2-\Phi_1)/2].\end{aligned} \tag{6}$$

This intensity is maximum if $|\Phi_2-\Phi_1|=0$ and minimum if $|\Phi_2-\Phi_1|=\pi$. Note that the intensity of the center frequency component can be considered to be constant, since the modulation depth is negligibly small ($J_0\{2m\cos[(\Phi_2-\Phi_1)/2]\}\approx 1$ for $m\ll 1$). This system is formally equivalent to a system providing constructive or destructive interference between the phase-modulated sidebands generated by Alice and Bob. One of the advantages is that no optical interferometric scheme is required.

Let us now consider the system operation when the laser diode is strongly attenuated. The output from a laser operating well above threshold can be described by a coherent state. The probability of observing a photocount with a detector at time t is proportional to $P_D = {}_D\langle\Psi|E^-(t)E^-(t)|\Psi\rangle_D$, with

$$E^-(t) = j\sum_{\omega} \xi(\omega)a_\omega \exp(-j\omega t), \tag{7}$$

$$E^-(t) = -j\sum_{\omega} \xi(\omega)a_\omega^- \exp(j\omega t), \tag{8}$$

$$\xi(\omega) = \left(\frac{\hbar\omega}{2\epsilon_0(2\pi)^3}\right)^{1/2}, \tag{9}$$

where ϵ_0 is dielectric permittivity of vacuum, a_ω and a_ω^- are the annihilation and creation operators, and $|\Psi\rangle_D$ is the coherent state describing the field incident on the detector. Initially, the quantum field emitted by the source is $|\Psi\rangle = |\alpha_{\omega_0}\rangle|0\rangle|0\rangle$ where two zero excitations are related to the two sidebands. At Alice's modulator output, the coherent state describing the quantum field can be deduced from Eq. (2) and by considering that the modulation depth m is sufficiently small tc obtain an average photcn number in the sidebands much smaller than 1. The coherent state at Alice's modulator output can then be written as a superposition of coherent states:

$$|\Psi\rangle_2 = |\alpha_{\omega_0}\rangle|\exp(-j\Phi_1)\alpha_{\omega_0-\Omega}\rangle|\exp(j\Phi_1)\alpha_{\omega_0+\Omega}\rangle. \tag{10}$$

Bob performs the same operation as Alice but introduces a phase Φ_2. Similarly, the state describing the quantum field at his modulator output is given by

$$|\Psi\rangle_3 = |\alpha_{\omega_0}\rangle|[\exp(-j\Phi_1) + \exp(-j\Phi_2)]\alpha_{\omega_0-\Omega}\rangle$$
$$\times|[\exp(j\Phi_1) + \exp(j\Phi_2)]\alpha_{\omega_0-\Omega}\rangle. \tag{11}$$

After spectral filtering, the state detected by the single photon detector is

$$|\Psi\rangle_D = |0\rangle|0\rangle|[\exp(j\Phi_1) + \exp(j\Phi_2)]\alpha_{\omega_0-\Omega}\rangle. \tag{12}$$

and the probability of photocount is proportional to

$$P_d = \langle\alpha_{\omega_0-\Omega}|(e^{-j\phi_1} + e^{-j\phi_2})$$
$$\times(e^{j\phi_1} + e^{j\phi_2})\sum_{\omega} \xi(\omega)a_\omega^- e^{j\omega t}$$
$$\times\sum_{\omega'} \xi(\omega')a_{\omega'}e^{-j\omega' t}\alpha_{\omega_0-\Omega}\rangle. \tag{13}$$

Recalling that $a_\omega|\alpha_{\omega'}\rangle = \alpha_\omega\delta_{\omega\omega'}$, we finally obtain

$$P_d = 4\xi(\omega)^2\cos^2[(\Phi_2 - \Phi_1)/2]\langle n_{\omega_0+\Omega}\rangle$$
$$= \rho\cos^2[(\Phi_2 - \Phi_1)/2], \tag{14}$$

TABLE I. Protocol for secret key transmission in the absence of an eavesdropper.

Bit sent by Alice	"0"		"1"	
Phase used by Alice	0		π	
Phase used by Bob	π	0	π	0
Photon detected by Bob	no	yes	yes	no
Bit received by Bob	?	0	1	?
Detection announced by Bob	no	yes	yes	no
Common bits shared		"0"	"1"	
Probability for photon detection	0	$\rho/4$	$\rho/4$	0

where $\langle n_{\omega_0-\Omega}\rangle = \langle\alpha_{\omega_0+\Omega}|a_{\omega_0+\Omega}^- a_{\omega_0+\Omega}|\alpha_{\omega_0+\Omega}\rangle$ is the average photon number at the detector in the sideband frequency $\omega_0+\Omega$, and ρ represents the probability of photocount per pulse, including the quantum efficiency of the detector. Equation (14) is formally equivalent to Eq. (6). Physically, Eq. (14) may be regarded as single photon interference that occurs at the FP output between the quantum fields of the side frequency $\omega_0+\Omega$ initiated by Alice and Bob. The probability of detecting a photon at the Fabry-Pérot output is 0 for $|\Phi_2-\Phi_1| = \pi$, $\rho/2$ for $|\Phi_2-\Phi_1| = \pi/2$, and ρ for $|\Phi_2-\Phi_1| = 0$. We show now how this property can be used to share a key.

III. PROTOCOL USED FOR QUANTUM KEY DISTRIBUTION

The protocol used is derived from the two-state scheme proposed by Bennett [3]. We shall describe the protocol in terms of the phase-encoded (these states should not be confused with the phase operator states of quantum optics) discussed in the preceding section. The nonorthogonal states used by Alice are formed by two states that differ by π, such as $\Phi_1 = 0$ for bit "0" and π for bit "1." Bob makes a measurement of each state he receives by using two phases that differ by π relative to those used by Alice, such as $\Phi_2 = \pi$ (then the bit read by Bob is "1" as a photon is detected) and 0 (bit "0"). The protocol can be described as follows.

(i) For each transmitted photon, Alice randomly chooses the state of transmission to be one of the two-phase states, namely 0 and π for bit "0" and bit "1," respectively. Every photon permits the transmission of a bit of information.

(ii) Bob randomly and independently chooses his measurement state (0 or π) for each incoming photon.

(iii) Bob then tells Alice, possibly over a public channel, the results of his measurements (photon detected or not), but not the phase that he used.

(iv) Alice and Bob agree to discard all the bits for which no photon was detected. In the absence of an eavesdropper, they now possess a shared random sequence of bits, which they could use as a secret key. Those first four steps are summarized in Table I. For instance, when Alice sends bit "0," the probability for Bob to detect a photocount is $\rho/4$, meaning that the probability to have the right bit "0" is also $\rho/4$.

If Eve is tapping the channel, because Eve cannot know which phases Alice and Bob will choose, there will, with certainty approaching unity, be times when Eve's choice re-

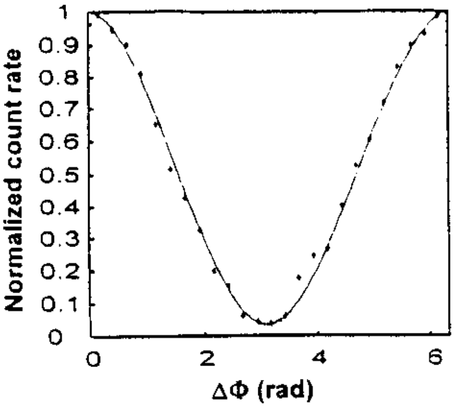


FIG. 5. Normalized single-photon count rate as a function of phase difference ΔΦ.

large compared with the intensity variation, which is 0.2, at the reference frequency component resulting from Alice's phase modulation. Hence, this intensity variation will be masked by the photon noise of the reference frequency and will not be detected by any intruder. It is then recommended to use a non-single-photon source and a very low modulation depth, instead of a single-photon source and a high modulation depth. Note that a very low modulation depth will also allow us to operate the modulators with very low driving voltages, making transmission in telecommunications systems at high bit rates easier.

Experiments in the quantum regime were performed by replacing the standard photodetector by a passively quenched germanium avalanche photodiode (APD) cooled to 77 K and operating with a photon counter in the Geiger mode. (Details of the APD characteristic will be described in another article devoted to photon counting at 1540-nm wavelength.) The DFB laser diode was modulated externally using an integrated intensity modulator to produce 50-ns-duration pulses at a repetition rate of 1 MHz. The pulses thus obtained were suitable for the photon counter we used. Note that the principle of operation described in Sec. II for a monochromatic source holds in the pulse regime, the phase difference $\Phi_2 - \Phi_1$ in Eqs. (6) and (14) being wavelength-independent. The mirror spacing of the FP was adjusted to obtain a spectral resolution of 36 MHz, a value that insures a 94% theoretical visibility. The carrier frequency Ω was 300 MHz. The DFB laser diode was attenuated to -80 dBm so that the average photon number μ of a side mode entering the transmission fiber was 0.1/pulse. The time response of the APD was 10 ns. The system was tested by measuring the visibility of the single-photon interference that occurs in the side frequency at the FP output. The visibility was measured varying $\Delta\Phi$ continuously between 0 and 2π rad with steps of 0.25 rad, and counting the photon number at the FP output. The photon counter was triggered with the initial light pulses and the duration of counting was set to be 50 ns. For each value of $\Delta\Phi$, measurement of the photon number was performed for 10^7 triggering pulses. For instance, with the modulators set in phase ($\Delta\Phi = 0$), we obtained an average number of 2500 counts, a value that corresponds approximately to 0.13 photon/pulse. Figure 5 shows the normalized average number of counts versus $\Delta\Phi$ thus obtained. The visibility calculated by subtracting dark counts is about 91%. Such a visibility corresponds to a quantum bit error rate (QBER) of 4%.

We note that the count rate, which was 250 counts/s, can be increased by using a higher modulation frequency, thereby allowing an increase in transmission rate. We did not try to optimize this parameter in these preliminary experiments.

V. CONCLUSION

In summary, we have reported a quantum cryptographic scheme involving single photon interference between phase-modulated sidebands produced by a pair of phase modulators in the transmitting and receiving modules. We conclude with some comments concerning the estimated performance and potential advantages of the scheme as compared with interferometer-based implementations.

(i) Polarization-independent behavior can be expected if the integrated $LiNbO_3$ phase modulators are replaced by intensity-modulating Mach-Zehnder interferometers [15]. When the input polarization fluctuates, the phase difference thus induced between the TE and TM modes in such modulators is shown to be small ($\approx\pi/30$). The resulting variation of the visibility of the single photon interference that occurs in the side frequency at the Fabry-Pérot output is negligibly small (<0.5%), meaning that QBER is expected to be constant if the polarization fluctuates in the transmitting fiber.

(ii) Because the modulators are quite compact, high stability against environmental thermal drifts can be obtained, as compared with that provided by a fiber Mach-Zehnder. The temperature of integrated modulators can be easily controlled to within 10^{-2} degrees. The corresponding variation in fringe visibility is smaller than 0.5% and does not alter the QBER significantly.

(iii) Since the physical principle of the scheme relies essentially on interference in the frequency domain, the most serious problems that may arise come from the possible instability of the wavelength emitted by the source, and of the frequency of the electrical signals produced by the VCO's, either of which can degrade system performance. As an example, if we use the same criterion as above (variation in fringe visibility <0.5%), calculations predict that a system operating with VCO's with a 5 GHz modulation frequency, and with a Fabry-Pérot with a finesse and a free spectral range of 100 and 100 MHz, respectively, requires the laser and the VCO frequency to be stabilized to within 10 and 5 MHz, respectively. Finally, it appears that the needed highly stabilized path-length differences in interferometer-based architectures translate in the proposed scheme into requirements for highly stabilized electronics devices.

(iv) The secret key is obtained by sacrificing some bits from raw data shared by Alice and Bob to improve security. The net secure throughput level of a two-state protocol is known to be smaller than with a four-state protocol [14]. We are investigating an improved version of the system to overcome this drawback.

ACKNOWLEDGMENT

We thank France Telecom for financial support.

[1] G. S. Vernam, J. Am. Inst. Electr. Eng. **XLV**, 109 (1926).

[2] C. H. Bennet and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Proceeding* (IEEE, New York, 1984), p. 175.

[3] C. H. Bennet, Phys. Rev. Lett. **68**, 3121 (1992).

[4] B. C. Jacobs and J. D. Franson, Opt. Lett. **21**, 1854 (1996).

[5] J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).

[6] A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1995).

[7] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).

[8] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 586 (1997).

[9] P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995).

[10] D. N. Klyshko, Phys. Lett. A **227**, 1 (1997).

[11] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[12] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[13] S. J. D. Phoenix and P. D. Townsend, Contemp. Phys. **36**, 165 (1995).

[14] B. Slutsky, R. Rao, P. C. Sun, and S. Fainman, Phys. Rev. A **57**, 2383 (1998).

[15] T. Ishikawa, Electron Lett. **28**, 566 (1992); C. C. Chen, H. Porte, A. Carenco, J. P. Goedgebuer, and V. Armbruster, IEEE Photonics Technol. Lett. **9**, 1361 (1997).