Pakistan Journal of Information and Technology 2 (3): 265-276, 2003
ISSN 1682-6027

Protocols for Secure Quantum Transmission: A Review of Recent Developments

Muhammad Musharraf Ishtiaq Khan and Muhammad Sher
Department of Computer Science, International Islamic University, Islamabad, Pakistan

Abstract: Data transmission has always been vulnerable to eavesdropping. Conventional cryptography has provided security in data communication, however it has some limitations when dealing with passive eavesdropping. Recently, the quantum mechanics has made a remarkable entry in the field of data communication. Now, it is possible to construct cryptographic communication systems which detect unauthorized eavesdropping and guarantee its prevention. Several protocols have been devised to implement such systems e.g., BB84, B92 and EPR. The famous BB84 protocol describes quantum encryption in terms of polarization states of a photon. The secret information is transmitted via secure quantum channel followed by a public conversation for verification and reconciliation. The B92 protocol is an extension of BB84 which shows how photons with non-orthogonal states can be used to distribute a secret key. The EPR protocol utilizes an entangled photon pair for encryption—one photon from this pair is transmitted towards the destination while keeping the other at the source; the destination photon describes the state of the source photon, failing to which confirms the intrusion. This paper presents a study of these protocols and a review on the recent developments in the field of secure quantum transmission.

Key words: Security, encryption, cryptography, eavesdropping, communication, quantum mechanics, protocols

Introduction

Secure transmission of information is a subject under discussion since ancient times. Especially in military applications, its importance is well-known. With the proliferation on internet and electronic mail, the importance of achieving secrecy in communications by cryptography—the art of using coded messages—is growing each day. Amazingly, quantum mechanics has now provided the foundation stone to a new approach to data encryption. It has been claimed that quantum encryption can solve many issues in data communication that are infeasible from the prospective of conventional cryptography.

Quantum mechanics, since introduced, has provided us with some very interesting concepts. The classical approach views the world as deterministic, where behavior of particles and systems is well defined. But now it is shown to be actually composed of a collection of particles whose behavior is probabilistic. In addition, we can actually never know the true state of a particle since measurement of one aspect of the state may perturb the value of other aspects of the state. This perturbation affect is known as the Heisenberg uncertainty principle and is the basis of some of the security issues presented by quantum communication systems.

Here we discuss some practical aspects behind the power of quantum cryptography. We will also explore some well-known protocols that describe the efficient use of quantum mechanics for secure data transmission. Finally, we will give some thoughts for the future.

Basics of quantum cryptography

Quantum mechanics describes a very basic phenomenon that relates with the polarization state of a single photon. Suppose a photon has four possible polarizations namely horizontal, vertical, 45 degrees and 135 degrees. We cannot distinguish between these four possibilities with certainty. This concept provides the foundation for the quantum encryption. We will consider the basic properties of quantum mechanics to understand this concept. First, there is a physical law in quantum mechanics known as the quantum 'no-cloning' theorem which states that an unknown quantum state cannot be cloned. Second, given a quantum system prepared in one of two prescribed non-orthogonal states, any attempt to distinguish between the two possibilities necessarily leads to disturbance. Third, a measurement on an arbitrary unknown quantum state is an irreversible process which introduces disturbance to the state. These three properties negate the possibility of passive monitoring of quantum signals. Therefore, eavesdropping on quantum channels necessarily disturbs the signal and is exceedingly likely to be detected. These properties are discussed in more detail.

Quantum no-cloning theorem

This theorem states that an unknown quantum state cannot be copied. The proof for this theorem is taken from (Hoi-Kwong, 1997). We will show by contradiction. Suppose a quantum Xerox machine exists and can copy an unknown state (Fig. 1). Considering the unitary evolution of the composite system with two orthogonal states |0, and |1,, respectively as the input, one finds that

$$|0, q\ |u, 6\ |0, q\ |0, q\ |v_0, \quad (1)$$

and

$$|1, q\ |u, 6\ |1, q\ |1, q\ |v_1, \quad (2)$$

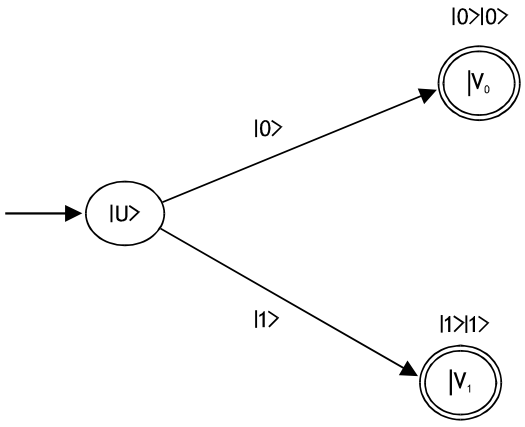

Fig. 1: A Xerox machine outputs a duplicate along with the original input

Where |u, is the initial state of the Xerox machine, $|v_0$, and $|v_1$, are the final states of the system excluding the original and the duplicate. $|v_0$, and $|v_1$, may be non-orthogonal. Now suppose that the input is, in fact, a linear superposition a|0, + b|1, (a, b … 0) of the two orthogonal states. Then by the linearity of quantum mechanics, one obtains from Eqs. (1) and (2) that

$$(a|0, + b|1,) q |u, 6 a|0, q |0, q |v_0, + b|1, q |1, q |v_1, \quad (3)$$

Notice that the state of the original is now entangled with the duplicate. However, for quantum cloning the resulting state should be a direct product

$$(a|0, + b|1,) q (a|0, + b|1,) q |vN, \quad (4)$$

Instead. Since

$$a|0, q |0, q |v_0, + b|1, q |1, q |v_1, … (a|0, + b|1,) q (a|0, + b|1,) q |vN, \quad (5)$$

whenever a, b … 0, one concludes that an unknown quantum state cannot be cloned.

Information gain implies disturbance

Another unusual property of quantum mechanics is that, in any attempt to distinguish between two non-orthogonal states, information gain is possible only at the expense of introducing disturbance to the signal. A proof is taken from (Hoi-Kwong, 1997) and goes as follow: Suppose we have a particle in one of two possible non-orthogonal states |N, and |4,. Also suppose that there is a quantum system in an initial prescribed state |u,. Assuming that the evolution leaves the state of the particle unchanged, we finds that

$$|N, q |u, 6 |N, q |v, \quad (6)$$

and

$$|4, q |u, 6 |4, q |vN, \quad (7)$$

where |v, and |vN, denote the final states of the quantum system in the two situations. Since the inner product is preserved by unitary transformations, we can take the inner product between the above two equations and finds that

$$(+u| q+N|)(|4, q |u,) = (+v| q +N|)(|4, q |vN,) +u|u, • +N|4, = +v|vN, • +N|4, 1 = +v|vN, \quad (8)$$

where Eq.(8) follows from the fact that +N|4, … 0 for non-orthogonal states. Therefore, we conclude that |v, is the same as |vN,. In other words, a process that does not cause disturbance to any two non-orthogonal states can pull out no information while distinguishing between the two states. Thus, information gain in distinguishing between two non-orthogonal states is possible only at the expense of disturbing the state of the system.

Irreversibility of measurements

The theorem of section 2.2 unleashes another aspect of quantum mechanics. We might think that we make a measurement and copies the result of that measurement. But this is not possible because the measurement will disturb the state of the signal. Consequently, the result of a measurement is different from the initial state and copying will be unfaithful. To understand this point, we will consider a photon in one of its four possible polarizations. A birefringent calcite crystal can be used to detect and distinguish with certainty between horizontally and vertically polarized photons. If a horizontally polarized beam of light is passed through this crystal, then the photons pass straight through it. On the other hand, if we pass a vertically polarized beam of light, then the photons are deflected to a new path. This fact is shown in Fig. 2(a) and Fig. 2(b). Photons originally in these two polarizations are, therefore, deterministically routed. However, a beam of light polarized at some other direction experiences a different behavior. According to the law of quantum mechanics, the photons with such polarization will have some probability of going into either beam Fig. 2(c). A photon will then be repolarized according to which beam it goes into and permanently forget its original polarization. For instance, a diagonally (i.e., 45-degree or 135-degree) polarized photon is equally likely to go into either beam, revealing nothing about its original polarization.

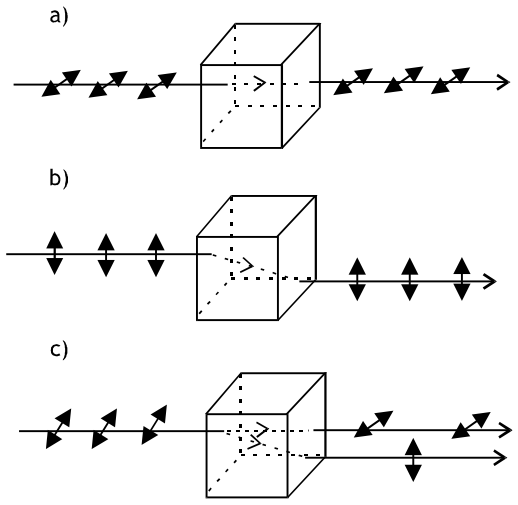

Fig. 2: A calcite crystal is used to distinguish between horizontal and vertical photons
(a) Horizontally polarized photons pass straight through
(b) Vertically polarized photons are deflected to a new path
© Diagonally polarized photons will have equal probability of coming our vertically or horizontally polarized

We can setup an apparatus to distinguish rectilinear (horizontal or vertical) photons by adding two detectors, such as photo multiplier tubes that can record single photons along the two paths, to the calcite crystal. By using this apparatus, an observer can reliably distinguish

between the two possibilities. This set up will, however, randomize the polarizations of diagonal (45- or 135-degree) photons, thus failing to distinguish between the two possibilities. In order to distinguish between diagonal photons, one should rotate the whole apparatus (calcite crystal and detectors) by 45 degrees. The rotated apparatus is, however, powerless in distinguishing between vertical and horizontal photons.

We can conclude from the above discussion that for a photon in one of the four polarizations (horizontal, vertical, 45-degree and 135-degree), a process of measure-and-copy will disturb the signal and fail to distinguish between the four possibilities. A measurement that distinguishes rectilinear photons will disturb diagonal photons. Similarly, a measurement that distinguishes diagonal photons will disturb rectilinear photons. This fundamental limitation in distinguishing between non-orthogonal states is due to the basic principles of quantum mechanics and thus it applies only to the particular measuring apparatus described here, but also to any measuring apparatus.

The BB84 quantum cryptographic protocol

BB84 protocol was proposed by Bennett and Brassard (1984). It is the first well known quantum cryptographic protocol. This protocol has been experimentally demonstrated to work for a transmission over 30 km of fiber optic cable (Phoenix, 1995) (Townsend, 1994) (Townsend and Thompson, 1994) (Townsend *et al.,* 1993) and also over free space for a distance of over one hundred meters (Jacobs, 1996 and Franson, 1994). Experiments for ground to satellite communication are also underway. It is speculated, but not yet experimentally verified, that the BB84 protocol should be implement able over distances of at least 100 km.

We now describe the BB84 protocol in terms of the polarization states of a single photon. A detailed description of this protocol is given in (Samuel, 1998). Fig. 3 illustrates the steps taken in this protocol.

Let H be the two dimensional Hilbert space whose elements represent the polarization states of a single photon. We can make use of two different orthogonal bases of H, namely circular polarization basis and linear polarization basis. The circular polarization basis consists of the kets $|\curvearrowright\rangle$, and $|\curvearrowleft\rangle$, for right and left circular polarization states, respectively. The linear polarization basis consists of the kets $|\updownarrow\rangle$, and $|\leftrightarrow\rangle$, for vertical and horizontal linear polarization states, respectively.

The BB84 protocol utilizes any two incompatible orthogonal quantum alphabets in the Hilbert space H. Let Au be the circular polarization quantum alphabet and Ar be the linear polarization quantum alphabet, as shown in Table 1 and Table 2, respectively.

Table 1: Circular Polarization Quantum Alphabet Au

Symbol	Bit
$\|\curvearrowright\rangle$,	1
$\|\curvearrowleft\rangle$,	0

Table 2: Linear Polarization Quantum Alphabet Ar

Symbol	Bit
|;,	1
|:,	0

Let us suppose that a key exchange is going to take place between two parties namely Ali and Omar and this communication is threatened by Khan—an eavesdropper. To assure the detection of Khan's eavesdropping, Bennett and Brassard require Ali and Omer to communicate in two steps, the first step over a one way quantum communication channel from Ali to Omer, the second step over a two way public communication channel.

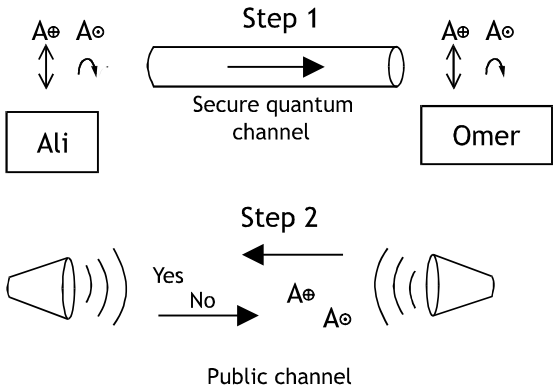

Fig. 3: Steps in BB84 protocol

Communication over a quantum channel

Ali randomly selects, each time he sends a bit, one of the two orthogonal alphabets Au or Ar with equal probability. Since no measurement operator of Au is compatible with any measurement operator of Ar, it follows from the Heisenberg uncertainty principle that no one, not even Omer or Khan, can receive Ali's transmission with an accuracy of greater than 75%, i.e. the minimum error rate is ¼.

With the knowledge put forward in section 2.3, a measurement that distinguishes linear photons will disturb circular photons. Similarly, a measurement that distinguishes circular photons will disturb linear photons. This shows that A_ and Ar are incompatible and because of this incompatibility, there is no simultaneous measurement operator for both Au and Ar. Since one has no knowledge of Ali's secret choice of quantum alphabet, 50% of the time (i.e., with probability ½) one will guess correctly, i.e., choose a measurement operator compatible with Ali's choice and 50% of the time (i.e., with probability ½) one will guess incorrectly. A correct guess means Ali's transmitted bit is received with probability 1. On the other hand, an incorrect guess means Ali's transmitted bit is received correctly with probability ½. Thus in general, the probability of correctly receiving Ali's transmitted bit is

$$P = ½ \bullet 1 + ½ \bullet ½ = ¾$$

Let 8 be the probability of Khan's eavesdropping, 0 # 8 # 1. Therefore, if Khan is not eavesdropping, then the probability will be 1 - 8. Thus, if 8 = 1, Khan is eavesdropping on each transmitted bit and if 8 = 0, Khan is not eavesdropping at all.

As discussed earlier, both Omer and Khan have no knowledge of Ali's choice of alphabet. Also, the measurement operators they choose are stochastically independent of each other. Therefore Khan's eavesdropping has an immediate and detectable impact on Omer's received bits. Khan's eavesdropping causes Omer's error rate to jump from ¼ to ¼ (1 - 8) + (3/8)8 = ¼ + 8/8

Thus, if Khan eavesdrops on every bit, i.e., if 8 = 1, then Omer's error rate jumps from ¼ to 3/8, a 50% increase.

Communication over a public channel

Ali and Omer communicate in two phases over a public channel to check for Khan's presence by analyzing Omer's error rate.

Extraction of raw key

This step is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Khan's eavesdropping (Fig. 4). Omer publicly communicates to Ali which measurement operators (not the results) he used for each of the received bits. Ali then in turn publicly communicates to Omer to tell him which of his measurement operator choices were correct. After this two way communication, Ali and Omer delete the bits corresponding to the incompatible measurement choices for which they can start over again later to communicate these bits securely. The sequence of bits obtained after deletion is known as the raw key. Both Ali and Omer have their own raw key which may differ with each other.

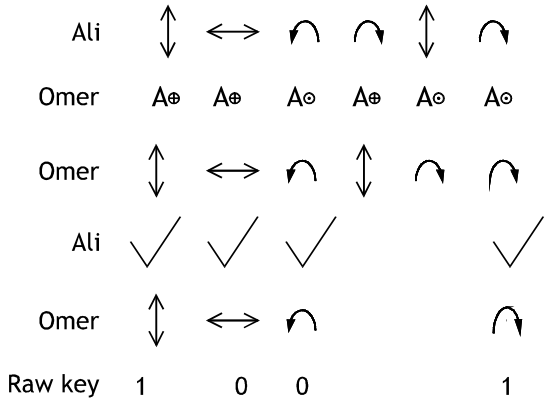

Fig. 4: Determination of Key using BB84 protocol

If there is no intrusion, then Ali's and Omer's raw keys will be in total agreement. However, if Khan has been at work, then corresponding bits of Ali's and Omer's raw keys will not agree with probability

$$0 \bullet (1 - 8) + ¼ \bullet 8 = 8/4$$

Detection of external intrusion via error detection

This step is dedicated to check for external intrusion e.g., Khan's presence. Ali and Omer select a publicly agreed upon random subset of m bit locations in the raw key and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed. In the absence of noise, if a comparison reveals an inconsistency, then Khan's eavesdropping has been detected, in which case Ali and Omer return to step 1 and start over. On the other hand, if no inconsistencies are uncovered, then the probability that Khan escapes detection is:

$$P_{false} = (1 - 8/4)^{m}$$

For example, if 8 = 1 and m = 200, then

$$P_{false} = (¾)^{200} . 10^{-25}$$

Thus, if P_{false} is sufficiently small, Ali and Omer agree that Khan has not eavesdropped and accordingly adopt the remnant raw key as their final secret key.

The B92 quantum cryptographic protocol

The B92 protocol was proposed by Bennett (1992). Like BB84 protocol, this protocol can be described in terms of any quantum system represented by a two dimensional Hilbert space. As described in (Samuel, 1998); we choose the two dimensional Hilbert space H representing the polarization states of a single photon.

B92 can be implemented in terms of any non-orthogonal basis. Let |N, and |n, be the kets representing the polarization state of a photon linearly polarized at an angle N and an angle n, respectively, with respect to the vertical, where 0 # N # B/4.

Unlike BB84 which requires two orthogonal quantum alphabets, B92 requires only a single non-orthogonal quantum alphabet. We choose the non-orthogonal quantum alphabet A_N, as described in Table 3.

Table 3: Linear polarization quantum alphabet A_N

Symbol	Bit
|N,	1
|n,	0

As in BB84, Ali and Omer communicate in two steps, the first over a one way quantum channel, the second over a two way public channel.

Communication over a quantum channel

Ali generates a random sequence of photons using the quantum alphabet A_N and sends it to Omer. Since $|N,$ and $|n,$ are not orthogonal, there are many experiments that unambiguously distinguish between these two polarization states. Thus, Omer can use one of many possible measurement strategies. Bennett (1992) suggests the measurements be based on the two incompatible experiments corresponding to the projection operators

$$P_{not\ N} = 1 - |N, +N| \text{ and } P_{not\ n} = 1 - |n, +n|$$

In this case, Omer either correctly detects Ali's transmitted bit, or an ambiguous result, i.e., an erasure, denoted by "?". Assuming that Ali transmits 0's and 1's at random with equal probability and that, for each incoming bit, Omer at random with equal probability chooses to base his experiment on either of the incompatible operators $P_{not\ N}$ or $P_{not\ n}$, then the probability of Omer's correctly receiving Ali's transmission is

$$(1 - || + N | n , ||^2) / 2$$

and the probability of receiving an erasure is

$$(1 + || + N | n , ||^2) / 2$$

where

$$|| + N | n , || = \cos (2N)$$

and where $0 < N < B/4$. Thus, Omer receives more than 50% erasures.

On the other hand Ekert (1994) suggest a more efficient measurement process for Omer. They suggest that Omer base his experiments on the positive operator valued measure (POVM) (Busch, 1991) (Peres, 1993) consisting of the operators

$$A_N = (P_{not\ N}) / (1 + || + N | n , ||),\ A_n = (P_{not\ n}) / (1 + || + N | n , ||) \text{ and } A_? = 1 - A_N - A_n$$

With this more efficient detection method, the probability of an inconclusive result is now

$$|| + N | n , || = \cos (2N)$$

where again $0 < N < B/4$

Communication over a public channel

Omer publicly informs Ali as to which time slots he received non erasures. The bits in these time slots become Ali's and Omer's raw keys. Khan's presence is detected by an unusual error rate in Omer's raw key. It is also possible to detect Khan's presence by an unusual erasure rate for Omer.

However, Ekert (1994) do point out that Khan can choose eavesdropping strategies which have no effect on the erasure rate and hence, can only be detected by unusual error rates in Omer's raw key.

EPR quantum cryptographic protocols

Ekert (1991) has devised a quantum protocol based on the properties of quantum correlated particles.

Einstein, Podolsky and Rosen (EPR) in their famous 1935 paper (Einstein, 1935) point out an interesting phenomenon in quantum mechanics. According to their theory, the EPR effect occurs when a pair of quantum mechanically correlated photons, called the entangled photons, is emitted from a source. The entanglement may arise out of conservation of angular momentum. As a result, each photon is in an undefined polarization. Yet, the two photons always give opposite polarizations when measured along the same basis. Since EPR pairs can be pairs of particles separated at great distances, this leads to what appears to be a paradoxical "action at a distance".

For example, it is possible to create a pair of photons (each of which we label below with the subscripts 1 and 2, respectively) with correlated linear polarizations. An example of such an entangled state is given by

$$|S_0, = 1/v2 (|0,_1 |B/2,_2 - |B/2,_1 |0,_2)$$

Thus, if one photon is measured to be in the vertical linear polarization state |0,, the other, when measured, will be found to be in the horizontal linear polarization state |B/2, and vice versa.

Einstein (1935) then state that such quantum correlation phenomena could be a strong indication that quantum mechanics is incomplete and that there exist "hidden variables", inaccessible to experiments, which explain such "action at a distance".

Bell (1964) gave a means for actually testing for locally hidden variable (LHV) theories. He proved that all such LHV theories must satisfy the Bell inequality. Quantum mechanics has been shown to violate the inequality.

The EPR quantum protocol is a 3**S**state protocol that uses Bell's inequality to detect the presence or absence of Khan as a hidden variable. We now describe a simplified version of this protocol in terms of the polarization states of an EPR photon pair.

As with the BB84 and B92, there are two steps to the EPR protocol, the first step over a quantum channel, the second over a public channel.

Communication over a quantum channel

An EPR pair is created at the source. One photon of the constructed EPR pair is sent to Ali, the other to Omer. Ali and Omer at random with equal probability separately and independently measure their respective photons. Ali records his measured bit. On the other hand, Omer records the complement of his measured bit. This procedure is repeated for as many EPR pairs as needed.

Communication over a public channel

Ali and Omer communicate over a public channel.

Separation of key into raw and rejected keys

Ali and Omer carry on a discussion over a public channel to determine the correct bases they used for measurement. They each then separate their respective bit sequences into two subsequences. One subsequence, called raw key, consists of those bits at which they used the same basis for measurement. The other subsequence, called rejected key, consists of all the remaining bits.

Detection of Khan's presence with Bell's inequality applied to rejected key

Unlike the BB84 and B92 protocols, the EPR protocol, instead of discarding rejected key, actually uses it to detect Khan's presence. Ali and Omer now carry on a discussion over a public channel comparing their respective rejected keys to determine whether or not Bell's inequality is satisfied. If it is, Khan's presence is detected. If not, then Khan is absent.

Quantum mechanics will have a dramatic impact on cryptographic communication systems. It is now within the realm of possibility to build practical cryptographic systems which check for, detect and prevent unauthorized intrusion. Quantum mechanics provides an intrusion detection mechanism never thought possible within the world of classical cryptography. Most importantly, the feasibility of these methods has been experimentally verified in a laboratory setting.

Much remains to be done before quantum cryptography is a truly practical and useful tool for cryptographic communication. We list below some of the areas in need of development:

- Quantum protocols need to be extended to a computer network setting.
- There is a need for greater understanding of intrusion detection in the presence of noise. The no cloning theorem and the "no detection implies no information" theorem simply do not provide a complete picture. (Ekert, 1994).
- There is a need for better intrusion detection algorithms. All quantum intrusion detection algorithms in the open literature depend on some assumption as to which eavesdropping strategy is chosen by Khan. It is important that eavesdropping algorithms be developed that detect Khan's intrusion no matter which eavesdropping strategy he uses.

It would be interesting to see if the quantum error correction can be used in practice to increase the range of quantum key distribution from the state-of-the-art tens of km to a

futuristic range of thousands of km. This would be an important milestone in the feasibility study of a practical quantum key distribution system.

References

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing, International conference on Computers, Systems and Signal Processing, Bangalore, India.

Bennett, C.H., 1992. Quantum cryptography using any two non-orthogonal states, Physical Review Letters, 68: 21.

Busch, P., P.J. Lahti and P. Mittelstaedt, 1991. The Quantum Theory of Measurement, Springer**S**Verlag, New York.

Einstein, A., B. Podolsky, N. Rosen, 1935. Can quantum, mechanical description of physical reality be considered complete?, Phys. Rev. 47, 1951. D. Bohm "Quantum Theory", Prentice**S**Hall, Englewood Cliffs, NJ.

Ekert, A.K., B. Huttner, G.M. Palma and A. Peres, 1994. Eavesdropping on quantum**S**cryptographical systems, Phys. Rev. A., 50: 2.

Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem, Physical Review Letters, 67: 6.

Franson, J.D. and H. Ilves, 1994. Quantum cryptography using polarization feedback, J. Modern Optics, 41: 12.

Hoi-Kwong Lo, 1997. Quantum Cryptology, Networked Systems Department, HP Laboratories Bristol.

Jacobs, B.C. and J.D. Franson, 1996. Quantum cryptography in free space, Optics Letters, Vol. 21.

Peres, A., 1993. Quantum Theory: Concepts and Methods, Kluwer Academic Publishers, Boston.

Phoenix, S.J. and P.D. Townsend, 1995. Quantum cryptography: how to beat the code breakers using quantum mechanics, Comtemporay Physics, 36: 3.

Samuel, J. and L. Jr., 1998. A quick glance at quantum cryptography, Dept. Comp. Sci. and Elect. Engr., Uni. Maryland Baltimore County.

Townsend, P.D., 1994. Secure key distribution system based on quantum cryptography, Electronic Letters, 30: 10.

Townsend, P.D. and I. Thompson, 1994. Journal of Modern Optics, A quantum key distribution channel based on optical fibre, 41: 12.

Townsend, P.D., J.G. Rarity and P.R. Tapster, 1993. Single photon interference in 10km long optical fibre interferometer, Electronic Letters, 29.