Abstract—With the growth of computer networks for business transactions and communication of confidential information there is an ever increasing need for encryption to ensure that this information cannot be acquired by third parties. Remarkably, the seemingly unrelated philosophical foundations of quantum mechanics are now being brought to bear directly on the problem of communications security in the potentially practical emerging technology of quantum cryptography. In this paper we shall review the theory of quantum cryptography, its potential applications and its use in optical fiber cable networks.

Keyword—Cryptography, Quantum Mechanics, QKD, Fiber optic.

1. INTRODUCTION

Throughout time information has been gathered, stored and communicated in various forms. The earliest means of information was visual, through diagrams and pictures. Languages were then developed and text became the major means of information management.

This continued until the information revolution in the early 20th century with the advent of the digital age. Electronic media propelled our society into an information driven society, however this has come with many complications, one being that of data integrity, privacy and secrecy [2]. The development of high-sensitivity, high-speed, and low noise photon detectors is called for as a key technology for quantum cryptography and quantum information and communications technology. This lead to the idea that using laser with that much energy would allow us to do communications with much larger information capacity; the quantum communication has taken its way to develop at a slow pace. However, the optical fiber at that time was not at a commercial stage. In the 1980s, the quantum communication faced a significant turning point. the quantum computer technology would radically affect the infrastructure of modern society.. The conventional optical communications can only control light as a flux of energy. the light has the characteristics of waves, and of particles.

When we are able to make use of the characteristics of the particles of light, namely, photon, we could realize quantum cryptography that can detect any fact of eavesdropping The act of eavesdropping means extracting a photon; the spot where a photon is taken away remains when the data is received, and thus the eavesdropping can be found out very easily. And when such a technology that can yield maximum
amount of information from each photon is created, the signal with same energy as before can convey much more information than before. the ultimate communications technology that can be allowed by the laws of physics is the quantum communication. [1]

2. NEED FOR CRYPTOGRAPHY

Cryptography defined as "the science and study of secret writing," concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes [2], ciphers [3], and other methods, so that only certain people can see the real message. it is about constructing and analyzing protocol that overcome the influence of adversaries [3] and which are related to various aspects in information securit such as data confidentialit, data integrit, authenticatio, and non-repudiatio. [4] Modern cryptography intersects the disciplines of mathematic, computer science, Cryptography prior to the modern age was effectively synonymous with encryptio, the conversion of information from a readable state to apparent nonsens. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same.

3. QUANTUM CRYPTOGRAPHY

Quantum cryptography describes the use of quantum mechanica effects (in particular quantum communication and quantum computatio) to perform cryptographi tasks or to break cryptographi systems. Quantum mechanics is a branch of physic dealing with physical phenomena at microscopic scales, where the actio is on the order of the Planck constan. Quantum mechanics provides a mathematical description of much of the dual particle-like and wave-like behavior and interactions of energ and matte. Electromagnetic waves such as light waves can exhibit the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter is a material that allows only light of a specified polarization direction to pass. If the light is randomly polarized, only half of it will pass a perfect filter. According to quantum theory, light waves are propagated as discrete particles known as photons. A photon is a massless particle, the quantu of the electromagnetic field, carrying energy, momentum, and angular momentu. The polarization of the light is carried by the direction of the angular momentum or spin of the photons. A photon either will or will not pass through a polarization filter, but if it emerges it will be aligned with the filter regardless of its initial state; there are no partial photons. Information about the photon's polarization can be determined by using a photon detector to determine whether it passed through a filter. [4] he foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. In particular, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements.

These characteristics provide the principles behind quantum cryptography. If an eavesdropper Eve uses a filter aligned with sender’s filter, she/he can recover the original polarization of the photon. But if receiver uses a misaligned filter she/he will
not only receive no information, but will have influenced the original photon so that she/he will be unable to reliably retransmit one with the original polarization. receiver will either receive no message or a garbled one, and in either case will be able to deduce Eve's presence.

Sending a message using photons is straightforward in principle, since one of their quantum properties, namely polarization, can be used to represent a 0 or a 1. Each photon therefore carries one bit of quantum information, which physicists call a qubit. To receive such a qubit, the recipient must determine the photon's polarization.

4. QUANTUM KEY DISTRIBUTION

Using quantum physics phenomena, we can build a perfectly secure key distribution system known as quantum key distribution (QKD). The quantum cryptography comprises the two steps of quantum key distribution and encryption by using the key. In the quantum key distribution, a key consisting of a random number sequence of "0" and "1", which is shared by those concerned in such a way that nobody other than the sender and receiver would possibly be able to eavesdrop it. This is a very simple system of adding the key to data at the ‘send’ and further adding the key at the ‘receive’ to recover the original data.

![Outline of quantum cryptographic system encryption](image)

A user can suggest a key by sending a series of photons with random polarizations. This sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail.

The sender of a key has to prepare a sequence of polarized photons – quantumbits (qbits), which are sent to the receiver through an optical fiber. In order to obtain the key represented by a given sequence of photons, the receiver must make a series of measurements using a set of polarization filters.

A photon can be polarized rectilinear (0°, 90°), diagonal (45°, 135°) and circular (left - spinL, right - spinR).

The process of mapping a sequence of bits to a sequence of rectilinearly, diagonally or circularly polarized photons is referred to as conjugate coding, while the rectilinear, diagonal and circular polarization are known as conjugate variables. Quantum theory stipulates that it is impossible to measure the values of any pair of conjugate variables simultaneously. The same impossibility applies to rectilinear, diagonal and circular polarization for photons. For example, if someone tries to measure a rectilinearly polarized photon with respect to the diagonal, all information about the photons rectilinear polarization is lost.

5. BB84 ALGORITHM OF QKD

BB84 is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984. BB84 allows two
parties, Sender and Receiver, to establish a secret, common key sequence using polarized photons – qbits. The steps in the procedure are listed below:

1. Sender generates a random binary sequence \( s \).
2. Sender chooses which type of photon to use (rectilinearly polarized, "R", or diagonally polarized, "D") in order to represent each bit in \( s \). Let \( b \) denote the sequence of each polarization base.
3. Sender uses specialized equipment, including a light source and a set of polarisers, to create a sequence \( p \) of polarized photons - qbits whose polarization directions represent the bits in \( s \).
4. Sender sends the qbits \( p \) to Receiver over an optical fiber.
5. For each qbit received, Receiver makes a guess of which base is polarized: rectilinearly or diagonally, and sets up his measurement device accordingly. Let \( b' \) denote his choices of basis.
6. Receiver measures each qbit with respect to the basis chosen in step 5, producing a new sequence of bits \( s' \).
7. Sender and Receiver communicate over a classical, possibly public channel. Specifically, Sender tells Receiver the choice of basis for each bit, and Receiver tells Sender whether he made the same choice. The bits for which Sender and Receiver have used different bases are discarded from \( s \) and \( s' \).

**Detecting Eavesdropper's presence**

For the \( i \)th bit chosen by Sender, \( s[i] \), there will correspond a choice of polarization basis, \( b[i] \), which is used to encode the bit to a photon. If Receiver 's chosen measurement basis is \( b'[i] \) and the outcome of his measurement is \( s'[i] \), then:

\[
b'[i] = b[i] \implies s'[i] = s[i]
\]

If an Eavesdropper tries to obtain any information about \( s[i] \), a disturbance will result and, even if Receiver and Sender 's bases match, \( s'[i] \neq s[i] \). This allows Sender and Receiver to detect the Eavesdropper's presence, and to reschedule their communications accordingly.[6]

**6. QUANTUM NETWORK**

QKD has been characterized by a dedicated two-point connection between endusers. This has served as a bottleneck towards the maturity of this research field into a commercially viable end product.

A two-node QKD setup has restricted applicative use due to the following reasons:

1. QKD is intrinsically limited in spatial coverage. This is mainly due to the absorption and dispersion of the qubit within the quantum channel.
2. The quantum key distribution rate is lower than its classical counterpart. Commercially viable products would require data rates comparable to present today cryptography.
3. The two-point QKD setup is prone to Denial of Service (DoS) attacks that isolate the end users. Hence a two-point setup would be considered frail.
4. The resources required for QKD far exceeds the product output. Hence the overhead capita is vastly increased when compared to classical cryptography.
Due to the dedicated fibre links between parties, mapping of key distribution relations is easily accessible. This may act as possible side information, thus compromising the provable security of the system. To counter the above bottlenecks, much research has been performed in the field of Quantum Networks (QN) in order to facilitate multi-user QKD on-demand with good Quality of Service (QoS).

A QN is a network that utilizes quantum mechanical principles to implement provably secure key transfer in a multi-node system. Such networks permit a hybrid of quantum channels to be integrated to form a complete network. The implementation of multi-user QKD over a fibre domain was spurred by the introduction of second-generation all-optical fibre networks. Previously fibre networks were opto-electrical, thus while the links between networking components and nodes were in the optical domain, the networking components converted optical signals to electrical pulses in order to manipulate or route the signal. The pulses are then converted back into the optical domain. These types of networks are unsuitable for QKD as the photons would be destroyed upon measurement by the components. All-optical, or second generation, networks use the properties of the light-pulses, eg the wavelength or intensity, to manipulate the pulses within the network. Thus the photon is not converted out of the optical domain and hence is not destroyed.

7. FIBER OPTIC IN QUANTUM NETWORK

Together with quantum enabled devices on both sender’s and receiver’s ends, QKD requires a medium through which such quantum information may be transferred. A quantum channel is a communication channel that can transmit quantum as well as classical information. A channel is defined as a linear, completely positive, trace preserving map [8]. This implies that:

- The channel maps positive operators to positive operators.
- The channel should preserve the normalization of states.
- The above results should apply when the channel maps the input to a sub-space of a higher dimensional space.

Many realizations of quantum channels exist. They vary from natural media, as in 1D magnets used as spin-chain quantum channels [9] to line-of-sight link in free-space through photon communication [10], to fabricated materials such as fibre optic cables. Optical Fibre as a Quantum Channel. Every implementation of a quantum channel is non-ideal due to its physical nature, however optical fibre has been found to be one of the most practical quantum channels available presently for photonic qubits. Single mode optical fibres act as a memoryless, noisy quantum channels.

Low attenuation and dispersion rectification are essential as the maximum key distribution distance and the detector gating windows, hence detector efficiency, are dependent on them respectively. Modern fibre is characterized by a low attenuation in the order of 0.2dB/km. Optical fibres further contain high bandwidths through multiplexing techniques permitting high-speed concurrent communication between multiple parties, this will assist the second generation QKD solutions to incorporate networking functionality. Optical fibre has a typical absorption spectrum with three transmission bands. The unique absorption characteristic is due to a superposition of Rayleigh backscattering, infrared absorption and certain molecule excitations [11].
As may be seen in Figure the third window at around 1550nm produces the least attenuation and is hence best suited for telecommunication and QKD.

Fig 4: absorption spectrum of optical fibre.

8. INTENDED RESEARCH IN QUANTUM NETWORK

The networking procedure outlined in the previous sections essentially facilitates network enabled QKD through a layer 3 implementation, however this still lacks some essential properties required for full commercial use. These, amongst others, include the financial viability for such implementations. the quantum nature of the key distribution has intrinsic and technical limitations. Through wavelength division multiplexed quantum networks many of the obstacles are overcome. However besides the technical complications of such an implementation further research is required in the following aspects:

1. Presently dark fibre is required for all available QKD systems. This is highly inefficient. A dark fibre used solely for classical cryptography could also enhance the security considerably through numerous parallel key exchanges and a complex function to derive a final key from the raw exchanged keys, this would provide for a much higher key production rate. The optimization of fibre capacity usage in QKD is dependent on the quality of the fibre as well as the networking components.

2. The quantum networks present today rely on trusted nodes to for the enhancement of spatial coverage. This however creates additional security vulnerabilities. In essence the proposals state that if the nodes of a network are sufficiently linked through entangled pairs, entanglement can be extended between any two nodes through unitary operations.

9. CONCLUSIONS

Quantum cryptography, or quantum key distribution (QKD), provides a means of unconditionally secure communication. The security is in principle based on the fundamental laws of physics. Security proofs show that if quantum cryptography is appropriately implemented, even the most powerful eavesdropper cannot decrypt the message from a cipher. Quantum cryptography has developed an entire field of research around itself merging together quantum mechanics and information theory to form Quantum Information Science. Its development has further been propelled by the rapid enhancement of quantum optics and fibre optic technology. Present technological challenges mainly revolve around detection efficiencies and fibre attenuation. These factors limit the rate and distance of quantum key distribution. The recent interest into the deployment of quantum networks have been to address factors that are hindering the mass commercialization of quantum cryptography. Most Quantum Key Distribution (QKD) protocols have a relatively low sifting efficiency, hence many successfully distributed qubits are left unused. The enhanced BB84 protocol is a minimally computer intensive, post-distribution algorithm that permits the recycling of qubits to enhance the efficiency of the original protocol. The key advantage of such a system is that no physical alterations are required to the
Further any implementation of the BB84 protocol can be enhanced.

ACKNOWLEDGEMENT

I am thankful to RGPV, Bhopal and Takshshila Institute of Engineering and Technology, Jabalpur for their valuable support during my work. I would also like to thank Prof Amit Agrawal for their valuable suggestions.

REFERENCES:


[2] A code is a system of communication that relies on a pre-arranged mapping of meanings such as those found in a codebook.

[3] A cipher is different from a code and it is a method of encrypting any text regardless of its content.


