QUANTUM CRYPTOGRAPHY

A thesis to be submitted by

Name: MOULI KAYAL

Reg. No. B2130142

Course Name : M 400

for the award of the degree of

MASTER OF SCIENCE

IN

MATHEMATICS

Under the supervision of

Prof. Stephan Baier

School Of Mathematical Sciences

RAMAKRISHNA MISSION VIVEKANANDA EDUCATIONAL AND RESEARCH INSTITUTE

BELUR MATH, HOWRAH, WEST BENGAL-711202,

21 JUNE, 2023

CERTIFICATE

This is to certify that the dissertation entitled **Quantum Cryptography** submitted by Mouli Kayal, for the partial fulfilment of the requirements for the degree of Masters of Mathematics in Ramakrishna Mission Vivekananda Educational and Research Institute. The above statement made by the candidate is correct to the best of my knowledge.

Date:.....

.....

Prof. Stephan Baier

Professor

Department of Mathematics

RKMVERI, Belur, Howrah

1 Acknowledgement

I would like to express my special thanks of gratitude to my guiding professor **Dr. Stephan Baier** , as well as other departmental professors who has given me the opportunity to do the dissertation on “Quantum Cryptography” which helped me to gather more knowledge in this field.

Signature Of The Student
Mouli kayal
Reg No : B2130142
M.Sc (4th Sem),
Department Of Mathematics ,
RKMVERI

Contents

1 Acknowledgement . . . 3
2 Abstract . . . 5
3 Introduction . . . 5
4 How Non Quantum Cryptography Works . . . 6
5 Limitations Of Non Quantum Cryptography . . . 7
6 Importance Of Quantum Resistant Cryptography . . . 9
7 Quantum Computers . . . 9
8 A Short Glossary Of Quantum Mechanics . . . 10
8.1 Heisenberg Uncertainty Principle . . . 12
8.2 Quantum Entanglement . . . 13
9 Ciphers . . . 14
9.1 Caesar Cipher . . . 14
9.2 Vernam's Cipher . . . 14
10 Quantum Key Distribution . . . 18
10.1 Qkd Protocols Using Heisenberg's Uncertainity Prinicples . . . 18
10.1.1 BB84 Protocol . . . 18
10.1.2 BB92 protocol . . . 21
10.1.3 SARG04 protocol . . . 21
10.1.4 Six-State protocol (SSP) . . . 22
10.2 Qkd Protocols Using Quantum Entanglement . . . 23
10.2.1 E91 protocol . . . 23
10.2.2 DPS protocol . . . 24
11 Discussion And Conclusion . . . 25
12 References . . . 26

2 Abstract

Modern cryptography algorithms are based over the fundamental process of factoring large integers into their primes, which is said to be "INTRACTABLE". But modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one-way functions such as that of factoring large integers. So the solution is to introduce quantum physics into cryptography, which lead to evaluation of quantum cryptography. Quantum cryptography is one of the emerging topics in the field of computer industry. This paper focus on quantum cryptography and how this technology contributes value to a defense-in-depth strategy pertaining to completely secure key distribution. The scope of this paper covers the weaknesses of modern digital cryptosystems, the fundamental concepts of quantum cryptography, the real-world implementation of this technology along with its limitations, and finally the future direction in which the quantum cryptography is headed towards. We describe results from an apparatus and protocol that is designed to implement the quantum key distribution by which two users who share no secret information (without having any private or public keys known before hand) initially exchange a random quantum transmission consisting of very faint flashes of polarized light.

3 Introduction

Quantum cryptography recently made headlines when European Union members announced their intention to invest 13 million dollar in the research and development of a secure communications system based on this technology. The system, known as SECOQC (Secure Communication based on Quantum Cryptography), will serve as a strategic defense against the Echelon intelligence gathering system used by the United States, Australia, Britain, Canada and New Zealand. In addition, a handful of quantum information processing companies, including MagiQ Technologies and ID Quantique, are implementing quantum cryptography solutions to meet the needs of businesses, governments, and other institutions where preventing the unauthorized disclosure of information has become a critical success factor in maintaining a competitive advantage over adversaries. While the modern cryptosystems are said to be very effective in other words they are said to be "INTRACTABLE" then why a lot of money is been spent to develop a new cryptosystem – quantum cryptography ?

4 How Non Quantum Cryptography Works

Before I get into Quantum Cryptography, I briefly have to tell you how the normal non quantum cryptography works, The one that most of the internet uses today . The cryptographic codes that are presently being used online are for the most part public key systems. the word "key" refers to the method that one uses to encrypt a message. it's basically an algorithm that converts readable text or data into a mess. But it creates this mess in a predictable way,so that the messing up can be undone. If the key is public, this means everybody knows how to encrypt a message, but only the reciepent knows how to decrypt it.This may sound somewhat perplexing because if the key is public and everybody knows how to scramble up a message , then it seems everybody also knows how to unscramble it . It does not sound very secure . But the clever part of Public Key Cryptography is that to encode the message you use a method that is easy to do but hard to undo.

For example you can compare it with a empty treasure chest in which you put your credit card number into it and close it,Now the rd to solve.There are various mathematical problems that can, and that are being used in cryptographic protocols for looking the treasure chest. The best known one is the factorization of a large number into primes, This method is used by the algorithm known as RSA.

RSA:- The idea behind RSA is based on the fact that it is difficult to factorize a large integer. RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Generating Public Key:

Step 1 : Choose two prime number p and q such that p not equal to q.

Step 2 : Calculate n = pq and $\phi(n)$ = (p-1)(q-1) .

Step 3 : Choose e such that $1 < e < \phi(n)$ and gcd(e,$\Phi(n)$) = 1 .

Hence the public key is (e,n) .

Generating Private Key:

Step 1: Consider the congruence equation $ex \equiv 1 \pmod{(\phi(n))}$

Step 2: Choose an integer d such that $ed \equiv 1 \pmod{(\phi(n))}$ (Using Extended Euclidean algorithm) .

Hence the private key is (d,n).

Mechanism Of The Algorithm:-

Encryption : Plaintext $\implies$ Ciphertext (Using Public Key)

Let m be the original message or plaintext . The public key is (e,n) . Let c be the encrypted message or ciphertext .

Then the encryption algorithm $c = m^e (mod n)$

Decryption : Ciphertext $\implies$ Plaintext (Using Private Key)

Let m be the original message or plaintext. The private key is (d,n) . Let c be the encrypted message or ciphertext . Then the decryption algorithm : $m = c^d (mod\ n\ )$

5 Limitations Of Non Quantum Cryptography

Now this public key can be broken in principle because we know algorithms to decompose numbers into their prime factor.But for large numbers these algorithms take very very long to give you a result,even on the world's presently most powerful computers.so may be that key you are using can be broken,after a hundred thousand years of computation time. But here is a thing whether or not someone can break one of these public keys depends on how quickly they can solve mathematical problem behind it and **Quantum Computers** can vastly speed up computation.You can see the problem Quantum Computers can break cryptographic protocols such as RSA in a short time and that is a big security risk.This is a problem which does not only affect your credit card number but really everything, from trade to national security.

Since public key cryptography involves complex calculations that are relatively slow, they are employed to exchange keys rather than for the encryption of voluminous amounts of data. For example, widely deployed solutions, such as the RSA and the Diffie-Hellman key negotiation schemes, are typically used to distribute symmetric keys among remote parties. However,

because asymmetric encryption is significantly slower than symmetric encryption, a hybrid approach is preferred by many institutions to take advantage of the speed of a shared key system and the security of a public key system for the initial exchange of the symmetric key. Thus, this approach exploits the speed and performance of a symmetric key system while leveraging the scalability of a public key infrastructure. However, public key cryptosystems such as RSA and Diffie-Hellman are not based on concrete mathematical proofs. Rather, these algorithms are considered to be reasonably secure based on years of public scrutiny over the fundamental process of factoring large integers into their primes, which is said to be "intractable". In other words, by the time the encryption algorithm could be defeated, the information being protected would have already lost all of its value. Thus, the power of these algorithms is based on the fact that there is no known mathematical operation for quickly factoring very large numbers given today's computer processing power. While current public key cryptosystems may be "good enough" to provide a reasonably strong level of confidentially today, there is exposure to a handful of risks. For instance, advancements in computer processing, such as quantum computing, may be able to defeat systems such as RSA in a timely fashion and therefore make public key cryptosystems obsolescent instantly. As another example, while the DES algorithm, which has a 56 bit key, was once considered to be secure, it is no longer thought of as such since advancements in technology have made it trivial to defeat. The fact that powerful computers may crack DES in a few hours served as a catalyst for the development of the replacement Advanced Encryption Standard. Hence, one area of risk is that public key cryptography may be vulnerable to the future technology developments in computer processing. Secondly, there is uncertainty whether a theorem may be developed in the future or perhaps already available that can factor large numbers into their primes in a timely manner. At present, there is no existing proof stating that it is impossible to develop such a factoring theorem. As a result, public key systems are thus vulnerable to the uncertainty regarding the future creation of such a theorem, which would have a significant affect on the algorithm being mathematical intractable. This uncertainty provides potential risk to areas of national security and intellectual property which require perfect security. In sum, modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one way functions such as that of factoring large integers. If a factoring theorem were publicized or computing became powerful enough to defeat public cryptography, then business, governments, militaries and other affected institutions would have to spend significant resources to research the risk of damage and potentially deploy a new and costly cryptography system quickly.

6 Importance Of Quantum Resistant Cryptography

Now we are nowhere near having a quantum computer that could actually do such a computation. But the risk that one could be built in the next decades is high enough so that computer scientists and physicists have thought of ways to make public key cryptography more secure.They have come up with various cryptographic protocols that cant be broken by Quantum Computers. This is possible by using protocols which rely on mathematical problems for which a quantum computer does not bring an advantage. This cryptgraphy, which is safe from quantum computers is called "Post Quantum Cryptography" or sometime "Quantum Resistant Cryptography".

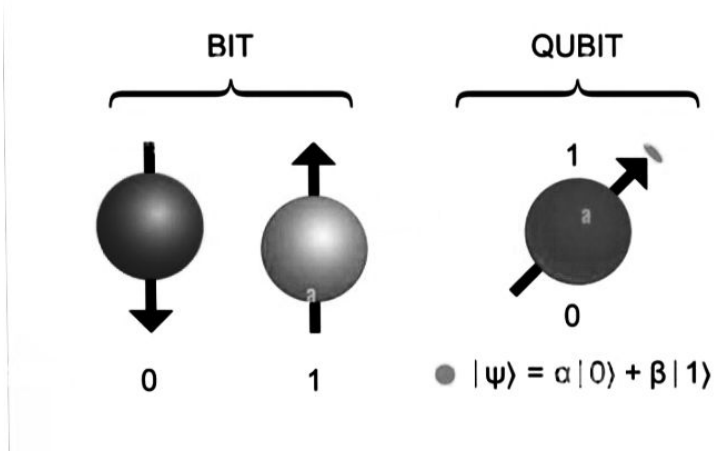
7 Quantum Computers

Quantum Computers Definition :-

A Quantum Computer is a computer that exploits quantum mechanical phenomena . At small scales, physical and quantum computing beverages this behaviour using specialized hardware .

How Does a Quantum Computer Work :-

A classical computer performs operations using classical bits which can be either 0 or 1 . Now in contrast a quantum computer uses quantum bits or qubits and they can be both 0 and 1 at the same time, and it is this that gives a Quantum Computer its superior computing power .



8 A Short Glossary Of Quantum Mechanics

Quantum Mechanics plays a key role in Quantum Cryptography, which refers to methods of secure communication that rely on the principles of quantum physics. In traditional Cryptography, security is based on mathematical algorithms, while in quantum cryptography it is based on the laws of physics. One of the most famous applications of quantum mechanics in quantum cryptography is the use of QKD protocols. these protocols allow two parties to share a secret key that can be used to encrypt and decrypt messages securely,even against a eavesdropper with unlimited computational power.QKD works by using the uncertainity principle of quantum mechanics to detect any attempts to intercept the key.

In this section we collect, without any claim of completeness , some basics of the mathematical machinery necessary to discuss quantum mechanics .

First of all, the mathematical setting is a real vector space H endowed with a scalar product $\langle , \rangle : \mathrm{H} \times \mathrm{H} \to \mathbb{R}$ with the property of being positive-definite, that is to say, such that $\langle u, u \rangle > 0$ for every non zero vector u $\in$ H . As usual, we also define the norm of a vector u $\in$ H as $\|u\| = \langle u, u \rangle$ and the length of u as $\mid u \mid = \sqrt{\|u\|} = \sqrt{\langle u, u \rangle}$

The vectors of length 1 are called unit vectors or versors . Two vectors u , v are said to be orthogonal if $\langle u, v \rangle = 0$

It is well known that in H there are orthonormal bases, that is, ordered pairs (u, v) of mutually orthogonal versors. Such pairs of vectors form a basis of H and allow us to identify H with $\mathbb{R}^2$ [with $\mathbb{C}^2$ in the complex case], by identifying the vector xu + yv with the ordered pair (x, y). Under this identification, the scalar product $\langle , \rangle$ is identified with the euclidean scalar $(x_1, y_1)(x_2, y_2) = x_1x_2 + y_1y_2$ [with the standard hermitian product $(x_1, y_1)(x_2, y_2) = x_1x_2 + y_1y_2$ in the complex case] . Of course, there are infinitely many orthonormal bases of H. However, suppose we have chosen one, by which we identify H with $\mathbb{R}^2$ as we just

explained: in other words, we introduced a coordinate system on H. This or- thonormal reference system is usually denoted by ($\uparrow$, $\rightarrow$), and its states cor- respond to vertically and horizontally polarised photons. We shall call this

reference frame rectilinear. Another natural orthonormal reference frame is the diagonal reference ($\nearrow$, $\searrow$), where $\nearrow$ and $\searrow$ correspond to the states of the photons polarised at 45 and 45 degrees with respect to the rectilinear reference, respectively. The connection between the two references is given by the following relations:

$$\begin{pmatrix} \nearrow \\ \searrow \end{pmatrix} = \frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} \uparrow \\ \rightarrow \end{pmatrix} = \frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

It is necessary now to formalise mathematically the notion of observation or measure of a photon . In our mathematical setting consisting of the vector space H , we shall call observable any linear mapping $A : H \to H$ that is symmetric [harmitian in the complex case]. namely such that for every pair of vectors $u, v \in H$ we have $\langle A(u), v\rangle = \langle u, A(v)\rangle$

We conclude this section giving a sketch of the mathematical formulation of Heisenberg uncertainty principle . First of all , some remarks about the product of two observables are in order . Given two observables A and B , we define their commutator [B,A] as the observable such that [B,A](v) := B(A(v)) - A(B(v)) for all v $\in H_c$. It is useful to remark that , for each pair of observables A , B , we have $\langle [B,A](v), v\rangle = \langle A(v), B(v)\rangle = \langle A(v), B(v)\rangle - \overline{\langle A(v) - B(v)} = 2Im(\langle A(v), B(v)\rangle) - - - - - - - - - - - - - (1)$

clearly we have [B,A] = 0 if and only if A and B commute that is to say , if and only if A $\cdot$ B = B $\cdot$ A , where the product is composition of mappings . Notice further that if A and B are observables , it is not always the case that A $\cdot$ B is an observable , but it is if A and B commute .

8.1 Heisenberg Uncertainty Principle

Heisenberg Uncertainty Principle:- Let A and B be observ- ables and let v be a state determined by a versor in H_c.*We have* $\triangle A(v)^2 \cdot \triangle B(v)^2 \geq \frac{1}{4}|\langle [B,A](v), v\rangle|^2 - - - - - - - - -(2)$

Ans:-

Notice that it suffices to prove the above for the observables A'= A - E(A)(v).I and B'= B - E(B)(v).I, where I is identity. Indeed, we have [B,A] = [B',A'],

$\triangle A(v) = \triangle$ A'(v) and $\triangle$ B(v) = B'(v).

Notice further that $E(A')(v) = E(B')(v) = 0$ *and so* $\triangle A'(v)^2 = \langle A'(v), A'(v)\rangle$ *and* $B'(v)^2 = \langle B'(v), B'(v)\rangle$ Therefore

$$|\langle [B', A'](v), (v)\rangle \ |$$

$= 2 \cdot |Im(\langle A'(v), B'(v)\rangle)| \leq 2|\langle A'(v), B'(v)\rangle|$.

We may conclude by applying cauchy − schwarz inequality

Notice that here it is actually important to consider everything in H_c rather than in H. Indeed if A and B are observables over H by (1) we have $\langle [B,A](v),(v)\rangle = 0$ for all v $\in$ H and Heisenberg uncertainty principle becomes trivial . Heisenberg principle becomes relevant for pair of observables A B such that $\langle [B,A](v),(v)\rangle = 2Im(\langle A(v),B(v)\rangle$ *is non zero for every versor* v. *In this case* , $((\langle [B,A](v),(v)\rangle)^2)/4$ *is a continuous function that never becomes zero on the compact set* $U = [v \in H_c : |v| = 1]$. *So it has a minimum* $M > 0$ *and equation* (2) *implies that* $\triangle A(v)^2.\triangle B(v)^2 \geq M$

8.2 Quantum Entanglement

The other important principle on which QKD can be based is the principle of quantum entanglement. It is possible for two particles to become entangled such [when a particular property is measured in one particle, the opposite state will be observed on the entangled particle instantaneously. This is true regardless of the distance between the entangled particles. It is impossible, however to predict prior to measurement what state will be observed thus it is not possible to communicate via entangled particles without discussing the observation over classical channel. The process of communicating using entangled states, aided by a classical information channel is known as quantum teleportation and is the basis of Eckerts protocol.

9 Ciphers

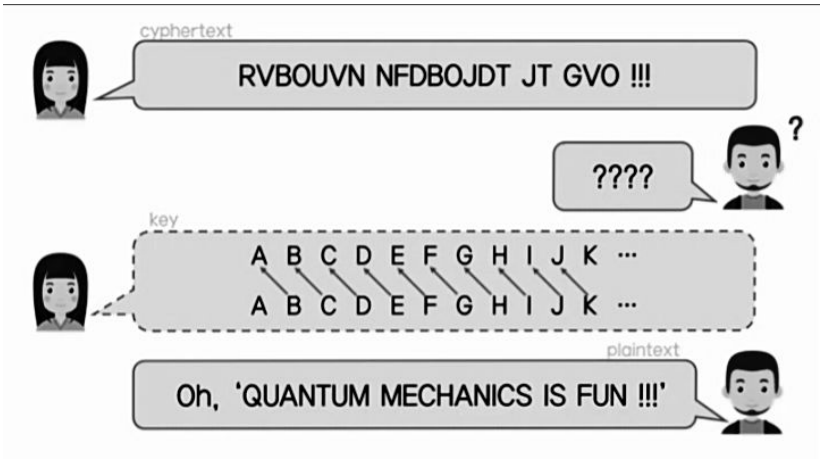
Ciphers:- Ciphers are also called encryption algorithms, are systems for encrypting and decrypting data . A cipher converts the original message called plaintext , into the ciphertext using a key to determine how it is done . That is in cryptography , A cipher is an algorithm for performing encryption or decryption .

9.1 Caesar Cipher

Caesar Cipher :-

The ceaser cipher technique is one of the earliest and simplest methods of encryption technique . It's simply a type of substitution cipher , i.e each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet . For example with a shift of 1 , A would replaced by B , B would become C , and so on . Tis method is apparently named after julius caesar who apparently used it to communicate with his officials . For example : if the right shift is 3 , the the letter A would be replaced by the letter D , B would become E , C would become F and so on .

Another Example:



9.2 Vernam's Cipher

Vernam's Cipher :- Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text.

Let m = m1m2 ...mr be a binary message to be sent. Let K = k1k2 ...kr be the key, which is a binary string of the same length of the message, consisting of random digits. The enciphering is carried out by substituting the message m with the message c = c1c2 ...cr, where

ci = mi + ki, i = 1, . . . r.

The key must not be used again. This cipher is called a Vernam's cipher. This cipher is also called **One time pad,** because the enciphering key used to be written on the sheets of a notepad to be made known to the users (the sender and the reciever) and should not be used more than one time.

Length of vernam cipher text is equal to the length of original text .

Example for enciphering:

plain text : Hello

Key : DGHBC

Then what is cipher text ?

ANS :

Numbering of letters position :

A	*B*	*C*	*D*	*E*	*F*
0	1	2	3	4	5
G	*H*	*I*	*J*	*K*	*L*
6	7	8	9	10	11
M	*N*	*O*	*P*	*Q*	*R*
12	13	14	15	16	17
S	*T*	*U*	*V*	*W*	*X*
18	19	20	21	22	23
Y	*Z*				
24	25				

Let us denote P = plain text ,

K = Key ,

C = Cipher text

then,

P =	H	E	L	L	O
	7	4	11	11	14
K =	D	G	H	B	C
+	3	6	7	1	2
	10	10	18	12	16
C =	K	K	S	M	Q

Hence the cipher text is KKSMQ .

Example for deciphering:

Let cipher text (C) = KKSMQ

Key (K) = DGHBC

Then what is plain text ?

ANS:

Numbering of letters position :

A	B	C	D	E	F
0	1	2	3	4	5
G	H	I	J	K	L
6	7	8	9	10	11
M	N	O	P	Q	R
12	13	14	15	16	17
S	T	U	V	W	X
18	19	20	21	22	23
Y	Z				
24	25				

Let us denote P = plain text ,

K = Key ,

C = Cipher text

then,

C =	K	K	S	M	Q
	10	10	18	12	16
K =	D	G	H	B	C
−	3	6	7	1	2
	7	4	11	11	14
P =	H	E	L	L	O

Hence the plain text is HELLO .

10 Quantum Key Distribution

Secret Key: According to the Vernam theorem, any message can be encoded in an absolutely secret way if the one uses a secret key of the same length.

The one who knows the key can decode the encoded message by adding the key to the message modulo 2. The important thing is that the key should be used only once. It is exactly this way that classical cryptography works.
Therefore the only task of quantum cryptography is to distribute the secret key between just two users (conventionally called Alice and Bob). This is Quantum Key Distribution (QKD). The sender sends these photons over a quantum channel to the receiver, who measures each photon's polarization and records the bit result. Since the photon's polarization is uncertain until it it is measured, an eavesdropper trying to intercept the key would inevitably disturb the photon and introduce errors in the measurement. Therefore, the two parties can check whether there is any error in their data which is due to interception and discard the compromised key bits.

10.1 Qkd Protocols Using Heisenberg's Uncertainity Prinicples

Quantum cryptography exploits the quantum mechanical property that a qubit cannot be copied or amplified without disturbing its original state . A compromised key in a QKD system is able to decrypt only a small amount of encoded information because of continuously changes in private key. A secret key can be build from a stream of a single photon where each photon is encoded with a bit value of 0 or 1, typically by a photon superposition state such as polarization. These photons are emitted by a conventional laser as pulses of dim light so that most pulses do not emit a photon. This approach ensures that few pulses contain more than one photon travel through the fiber-optic line. In the end only a small fraction of the received pulses actually contains a photon [28]. The photons that are reached to the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon.

10.1.1 BB84 Protocol

BB84 Protocol:
BB84 protocol is a quantum key distribution protocol, which means it allows two parties to share a secret key that can be used for encryption and decryption of messages. The protocol is named after its inventors Charles Bennett and Gilles Brassard, and is one of

the earliest and most widely implemented quantum key distribution schemes.
The idea is to encode every bit of the secret key into the polarization state of a single photon. Because the polarization state of a single photon cannot be measured without destroying this photon, this information will be " fragile " and not available to the eavesdropper. Any eavesdropper (called Eve) will have to detect the photon, and then she will either reveal herself or will have to re-send this photon. But then she will inevitably send a photon with a wrong polarization state. This will lead to errors, and again the eavesdropper will reveal herself.

The BB84 protocol works by using the properties of quantum mechanics to create a shared key that is completely secure from interception.
To translate photons bit into a key Photon with horizontal and A-diagonal spin means 1 and vertical and D-diagonal this spin means 0

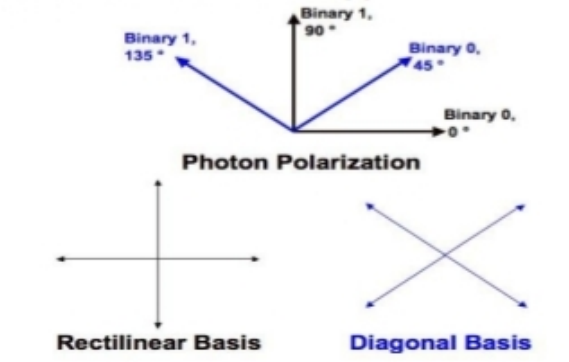


Figure 2: BB84 Bit Encoding

Let's assume alice wants to send very simple very simple 8 bits size message . She then randomly selects one of two filters for each qubit . Now each photons is having particular polarization state depending both on the beat values and selected filters and these photons transmitted to BOB through quantum channel . Bob does not know what filter does Alice choose so all he can do is to select it randomly he does this for each photon visit after the final direction of photons is observed . He communicates with Alice over the public quantum channel what filter they have chosen .They both discard photon measurements where Bob used a different filter with Alice which is happen every remaining half will be used as a shared key .
Notice that, in doing so, Bob might or might not make some error. Indeed, if he uses the filter + [the filter x , resp.] on a photon having rectilinear [diagonal, resp.] polarisation, no error occurs. But if he uses the filter + [the filter x , resp.] on a photon having diagonal [rectilinear, resp.] polarisation, this modifies the reception of the corresponding photon. As both the polarisation of the photons sent by Alice and the filters used by Bob are

randomly chosen, we may expect such errors to occur with probability 1/2. But these errors do not necessarily imply an error in the final received message. Indeed, for each error caused by using the wrong filter on one of Alice's photons, there is an even chance that the corresponding digit is the right one, although the polarisation of the photon is wrong.

- If there is no eavesdropper the probability P of Bob recieving correctly the message is
  $P = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} = 75\%$

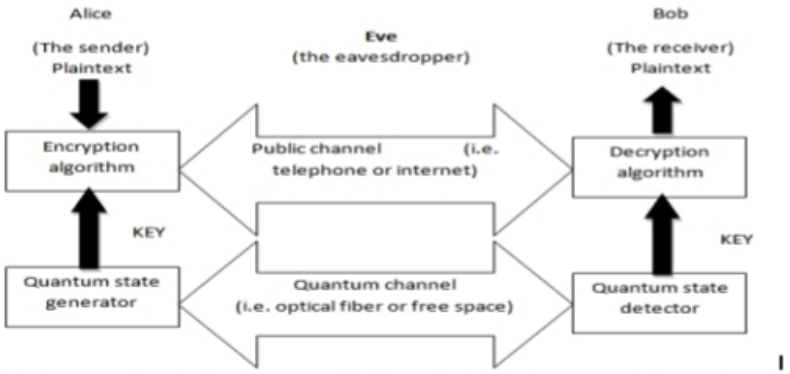


Figure 1: Quantum cryptographic communication System for securely transferring Random key

As Eve has no knowledge of the filter used in encoding by Alice , She can only guess like Bob . If she choose same filter as Alice She will measure the correct photon polarization state sent by Alice with 50 percent of probability . However even if she choose it incorrectly there is still 50 percent of probability to select the correct bit 0 or 1 .

The total probability of accurate transmission is submit 5 percent . If the result of transmission is different Alice and Bob can notice there is an eavesdropper . It seems like we only have 25 percent chance to catch the eavesdropper .
$P_d = 1 - \frac{3}{4}$
However if Alice and Bob publicly compare n numbers of their key bits the probability they find disagreement and identify the presence of Eve is this value as n gets larger the probability which is nearly 1 that means they can detect eavesdropper definitely .
$P_d = 1 - (\frac{3}{4})^n \approx 1$

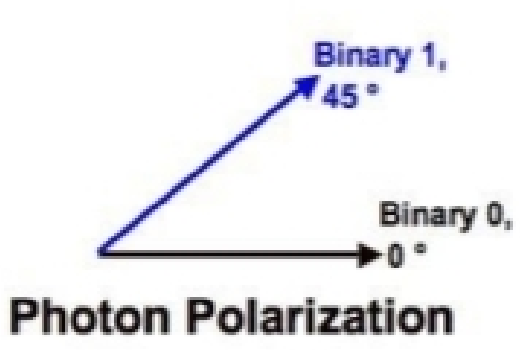
Assume Eve interferes with probability s with s lying between 0 and 1, that is, s is the proportion of photons Eve tampers with when eavesdropping on Alice and Bob . If $s = 0$, this means that Eve never interferes, while $s = 1$ means that Eve measures every photon Alice sends to Bob . Intermideate values of s mean that Eve sometimes listens on, sometimes does not . Due to the randomness hypotheses we made, Bob's and Eve's

choices when using filters are independent of each other and of the polarisations chosen by Alice when sending photons, so an error in the message received by Bob may occur only if : Bob is wrong , Which as we know happens with probability $\frac{1}{4}$, and Eve does not interfere , which has a probability equal to $1 - s$; Bob is correct, which happens with probability $\frac{3}{4}$, but Eve interferes with probability s , and causes an error in the choice of the filter , which in turn causes an error in the received message with probability $\frac{1}{2}$. In conclusion, the new error probability P' when Bob receives the message is given by the the formula P' = $\frac{1}{4}$ $(1 - s)$ + $\frac{3}{4}$ $\cdot\frac{1}{2}$ s = $\frac{1}{4} + \frac{s}{8}$

10.1.2 BB92 protocol

Soon after BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal basis for encoding and decoding. It turns out that a single non-orthogonal basis can be used instead, without affecting the security of the protocol against eavesdropping. This idea is used in the BB92 protocol, which is otherwise identical to BB84 protocol. The key difference in BB92 is that only two states are necessary rather than the possible 4 polarization states in BB84 protocol.

As shown in figure 3, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84 protocol, Client A transmit to Client B a string of photons encoded with randomly chosen bits but this time the bits Client A chooses dictates which bases Client B must use. Client B still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Client B can simply tell Client A after each bit Client B sends whether or not he measured it correctly.



10.1.3 SARG04 protocol

The SARG04 protocol is built when researcher noticed that by using the four states of BB84 with different information encoding they could develop a new protocol which

would more robust when attenuated laser pulses are used instead of single- photon sources. SARG04 protocol was proposed in 2004 by Scarani . The SARG04 protocol shares the exact same first phase as BB84. In the second Phase when Client A and Client B determine for which bits their bases matched, Client A does not directly announce her bases rather than Client A announces a pair of non-orthogonal states one of which she used to encode her bit. If Client B used the correct basis, he will measure the correct state. If he chose incorrectly he will not measure either Client A states and will not be able to determine the bit. If there are no errors, then the length of the key remaining after the sifting stage is $\frac{1}{4}$ of the raw key. The SARG04 protocol provides almost identical security to BB84 in perfect single-photon implementations: If the quantum channel is of a given visibility (i.e. with losses) then the QBER of SARG04 is twice that of BB84 protocol, and is more sensitive to losses. However SARG04 protocol provides more security than BB84 in the presence of PNS attack, in both the secret key rate and distance the signal can be carried (limiting distance).

10.1.4 Six-State protocol (SSP)

The 6-state or 3 bases cryptographic is nothing but the well-known BB84 4-state scheme with an

additional basis . Six-State Protocol (SSP) is proposed by Pasquinucci and Gisin in 1999.

When represented on the Poincare sphere the BB84 protocol makes use of four spin-1/2 states corresponding to

$\pm$x and $\pm$y direction. In brief summary Client A sends of the four states to Client B, who measures the qubits he

receives in either the X or Y basis. A priori this gives a probability $\frac{1}{2}$ that Client A and Client B use the same basis. On an average Client A and Client B have to discard half of the qubits even before they can start extracting their cryptographic key. In the 6 state protocols the two extra states correspond to $\pm$z, i.e. the 6 states are $\pm$x, $\pm$y, and $\pm$z on the Poincare sphere. In this case Client A sends a state chosen freely among the 6 and Client B measures either in the x, y or z-basis. Here the prior probability that Client A and Client B use the same basis is reduced to 1/3, which means that they have to discard 2/3 of the transmitted qubits before they can extract a cryptographic key. However, this scheme does hold an advantage compared to the BB84 protocol – higher symmetry. As it will be seen this fact together with the use of symmetric eavesdropping strategies dramatically reduced the number of free variables in the problem under investigation.

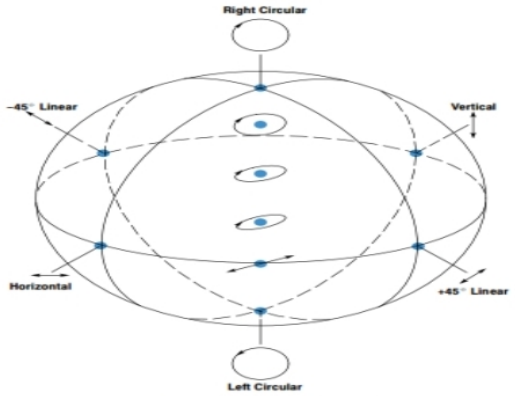


Figure 4: Poincare sphere

10.2 Qkd Protocols Using Quantum Entanglement

10.2.1 E91 protocol

The Ekert scheme uses entangled pairs of photons . These can be created by created by Client A, by Client B, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Client A and Client B each up with one photon from each pair. The Scheme relies on two properties of entanglement. First the entangled states are perfectly correlated in the sense that if Client A and Client B both measure whether their particles have vertical or horizontal polarizations, they will always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarization However the particular results are completely random, it is impossible for Client A to predict if and Client B will get vertical polarization or horizontal polarization. Second any attempt at eavesdropping by Eve will destroy these correlations in a way that Client A and Client B can detect.
The measurement in the figure 5 is divided into two groups; the first is when different orientations of the analyser were used and the second when the same analyser orientation was employed. Any photon which was not registered is discarded. Alice and Bob then reveal the result of the first group only, and check that they correspond to the value expected from Bells inequality. If this is so then Alice and Bob can be sure that the results they obtained in the second group are anti-correlated and can be used to produce a secret key string. Eve cannot obtain any information from the photons when they are transit as there is simple no information there. Information is only present once the authorized user performs their analyser measurements and key sifting. Eves only hope is to inject her own data for Alice and Bob, but as she doesnt know their analyser orientations, she will always be detected (the Bells inequality value will be too low).

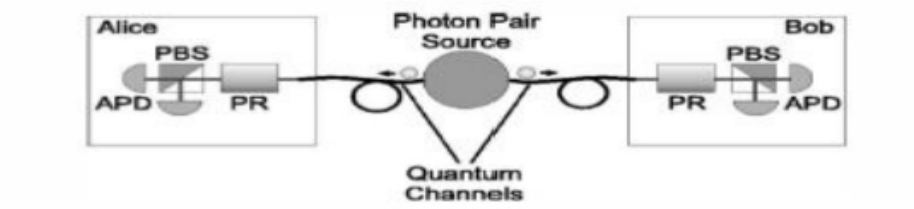


Figure 5: A Typical System Using Entangled Photon Pairs [35]

10.2.2 DPS protocol

Differential –phase-shift QKD (DPS-QKD) is a new quantum key distribution scheme that was proposed by K.Inoue .

Alice randomly phase-modulates a pulse train of weak coherent states by 0, for each pulse and sends it to Bob with an average photon number of less than one per pulse. Bob measure the Phase difference between two sequential pulses using a 1-bit delay. Mach-Zehnder interferometer and photon detectors, and records the photon arrival time and which detector clicked. After transmission of the optical pulse train, Bob tells Alice the time instances at which a photon was counted. From this time information and her modulation data. Alice knows which detector clicked at Bobs site. Under an agreement that a click by detector 1 denotes "0" and click by detector 2 denotes "1", for example Alice and Bob obtain an identical bit string. The DPS-QKD scheme has certain advantageous features including a simple configuration, efficient time domain use, and robustness against photon number splitting attack .

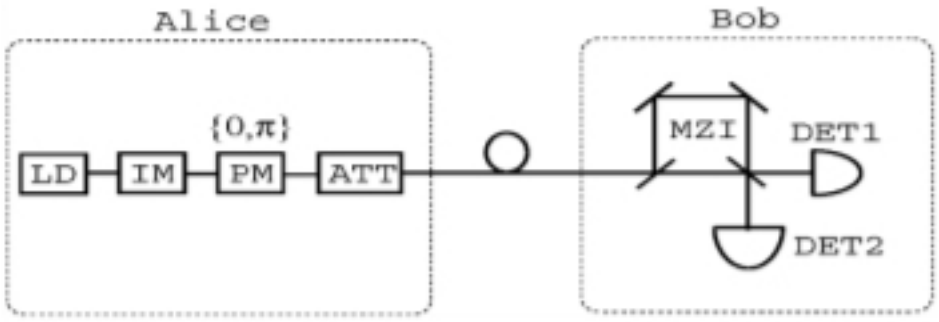


Figure 7: Schematic diagram of DPS protocol [38]

11 Discussion And Conclusion

DARPA is now starting to build multiple QKD links woven into an overall QKD network that connects its QKD endpoints via a mesh of QKD relays or routers. When a given point-to-point QKD link within the relay mesh fails – e.g. fiber cut or too much eavesdropping or noise abandons that link abandoned and another used instead. This emerging DARPA Quantum Network can be engineered to be resilient even in the face of active eavesdropping or other denial-of-service attacks. Such a design may be termed a "key transport network." Looking to the later years of the DARPA Quantum Network, the principal weakness in untrusted QKD networks – limited geographic reach – may perhaps be countered by quantum repeaters. There is now a great deal of active research aiming towards such repeaters, and if practical devices are ever achieved, they should slide neatly into the overall architecture of untrusted QKD networks to enable seamless QKD operations over much greater distances than currently feasible. A proposed solution to the distance problem may be to "chain" quantum cryptography links with secure intermediary stations. Otherwise, an alternative solution is transmission through free space or low orbiting satellite. In this scenario, the satellite acts as the intermediary station, and there is less attenuation of photons in the atmosphere. Research into this area is still ongoing and work is underway in both the US and Europe to be able to send quantum keys up to satellites and then down to another destination securely. While there have been substantial advancements in the field of quantum cryptography in the last decade, there are still challenges ahead before quantum cryptography can become a widely deployed key distribution system for governments, businesses, and individual citizens. Namely, these challenges include developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. However, the advances in computer processing power and the threat of obsolescence for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography. In fact, in is expected that nearly 50 million of both public and private funds will be invested in quantum cryptography technology over the next three years3. Quantum cryptography is still in its infancy and so far looks very promising. This technology has the potential to make a valuable contribution to e-commerce and business security, personal security, and security among government organizations. If quantum cryptography turns out to eventually meet even some of its expectations, it will have a profound and revolutionary affect on all of our lives.

12 References

1] M.W Baldoni, C.Ciliberto, G.M. Piacentini Cattaneo,
Elementary Number Theory , Cryptography and codes
2] Federico Grasselli ,
Quantum Cryptography From Key Distribution To Conference Key Agreement
3] Nirbhay Kumar Chaubey and Bhavesh B. Prajapati,
Quantum Cryptography And The Future Of Cyber Security