# CONTENTS

# ABSTRACT

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed due to wave function collapse (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution.

A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.

Cryptography was the method of encrypting the data with a key and decoding it at the receiving end to protect it from attacks of cybercrimes. With the same logic, let us try and define quantum cryptography- if the technique used to encrypt the plaintext is the principle of quantum mechanics then it is called quantum cryptography. It takes advantage of the 'no change theory' that means it cannot be interrupted knowingly or unknowingly.

The security of online transactions assumes the impossibility of factoring large numbers in a reasonable time using classical algorithms.

# CHAPTER 1

## 1.1 INTRODUCTION

Quantum cryptography is a new technique of securing computer network communication channel. Existing standard crypto systems are using advanced algorithms to create key pairs which are extremely hard to inverse engineer. Quantum cryptography avoids any mathematical algorithm and uses principles of quantum physics.

Quantum crypto implements a new technique of generating and exchanging crypto keys which makes it impossible for third party entities to get those keys by snooping or to create man in the middle by snooping and sending copies of original key. Keys generated in this way will automatically destroy themselves if read by third-party interferer. When generated between two sides, using quantum key distribution, secret keys will be used with standard and well known symmetric encryption. The key generation process is the only part which uses quantum principles to work, from there, using this "hyper-secure key" already existing symmetric encryption will be used to encrypt and decrypt data, which will be sent over standard, currently available, optic data networks.

Quantum cryptography usually uses photons to generate the key by sending pieces of data between two sides. It uses of course standard optic communication channel used in computer networks today. So we see that the mechanism is not only transmitting the key using photon polarization, but the process of sending polarized photons is actually the process which generates the key.

## 1.2 MOTIVATION

- Communication channels are spying on our data.
- Communication channels are modifying our data
- The world wide implementation of this can take up lots of jobs and hence unemployment will increase.

## 1.3 PROBLEM STATEMENT

The aim of this project is to provide an security to the secret messages. Despite all of the security it offers, quantum cryptology also has a few fundamental flaws. Chief among these flaws is the length under which the system will work: It's too short.

The original quantum cryptography system, built in 1989 by Charles Bennett, Gilles Brassard and John Smolin, sent a key over a distance of 36 centimetres [source: Scientific American]. Since then, newer models have reached a distance of 150 kilometres (about 93 miles). But this is still far short of the distance requirements needed to transmit information with modern computer and telecommunication systems.

The reason why the length of quantum cryptology capability is so short is because of interference. A photon's spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be. This means that a 1 may come through as a 0 -- this is the probability factor at work in quantum physics. As the distance a photon must travel to carry its binary message is increased, so, too, is the chance that it will meet other particles and be influenced by them. One group of Austrian researchers may have solved this problem. This team used what Albert Einstein called "spooky action at a distance." This observation of quantum physics is based on the **entanglement** of photons. At the quantum level, photons can come to depend on one another after undergoing some particle reactions, and their states become entangled. This entanglement doesn't mean that the two photons are physically connected, but they become connected in a way that physicists still don't understand. In entangled pairs, each photon has the opposite spin of the other -- for example, ( / ) and ( ). If the spin of one is measured, the spin of the other can be deduced. What's strange (or "spooky") about the entangled pairs is that they remain entangled, even when they're separated at a distance. The Austrian team put a photon from an entangled pair at each end of a fiber optic cable. When one photon was measured in one polarization, its entangled counterpart took the opposite polarization, meaning the polarization the other photon would take could be predicted. It transmitted its information to its entangled partner. This could solve the distance problem of quantum cryptography, since there is now a method to help predict the actions of entangled photons.

## 1.4 OBJECTIVES

Until fairly recently, the Information and Communication Technology (ICT) industry has considered information interchange transactions across electronic networks to be secure when encrypted using what are considered to be an unbroken conventional cryptographic system. Recent research in the field of quantum computing has produced a credible and serious threat to this assumption. Some problems that are considered difficult or impossible to solve using conventional computation platforms become fairly trivial for a quantum computer. Any information that has been encrypted, or will be encrypted using many of the industry's state-of-the-art cryptosystems based on computational hardness is now under threat of both eavesdropping and attack by future adversaries who have access to quantum computation. This means that even encrypted information sitting in a database for 25 years for example will be subject to discovery by those with access to quantum computing platforms. The discovery of the content of such data could lead to very serious consequences. These include the misuse of bank account numbers, identity information, items relating to military security and other sensitive information. **Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure.** The primary objective is to help raise awareness of the potential impacts of quantum computing on information security globally. This includes a 1) survey of current cryptographic principles, 2) the possible impact of quantum computing on their effectiveness and 3) what can be done to mitigate the risks in an economically and technically practical manner. We further include discussion of the enablers of quantum safe cryptographic techniques along with the realistic economic and technical challenges to its deployment in existing systems and the impact of global standards.

## 1.5 SUMMARY

Recent research in the field of quantum computing and quantum information theory has brought about a credible threat to the current state-of-the-art for information protection.

The current data protection mechanisms that typically comprise cryptographic systems rely on computational hardness as a means to protect sensitive data. This is to say that there are cryptographic problems that are difficult or impossible to solve using conventional computing. Because of recent advances in quantum computing and quantum information theory, the quantum

computer presents a serious challenge to widely used current cryptographic techniques. This is because some of the same cryptographic problems, which are difficult or impossible to solve using conventional computing, become fairly trivial for the quantum computer. In the practical case, even encrypted information sitting in a database for 25 years, for instance, will be subject to discovery by those having access to quantum computing platforms. The discovery of the content of such data may lead to serious consequences. These include the possible misuse of bank account numbers, identity information, items relating to military security and other sensitive

information. The current state-of-the-art cryptographic principles use well-studied methods that have been relied upon for more than 20 years. Amongst cryptographic experts, well-studied, proven and mature techniques are the most preferred for security reasons. However, such techniques were not designed to resist quantum attacks, because at the time of their invention, research into quantum computation was obscure and unknown to most cryptographic practitioners. New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed "quantum safe" and consist of both techniques based on quantum properties of light that prevent interception of messages, as well as classic computational techniques, all of which were designed to resist quantum attacks emerging from the rapidly accelerating research field of quantum computation. Cryptographic techniques are commonly found in many industries and fielded systems, usually as a component of broader network security products. These commonly available security products need to be upgraded with quantum safe cryptographic techniques, and this paper explores some of the most

pervasive security systems while giving practical recommendations for upgrading to a quantum safe state. This is not a trivial undertaking, and requires the interest and support of security product vendors, industry customers, academic researchers, and standards

groups. An important consideration is the cost of transitioning to quantum safe technologies. New products and

trends tend to follow a standard cycle of innovation starting with early adopters who pay high

premiums, and ending with commoditized product offerings with abundant competition. Quantum safe features will reset the innovation cycle for many common commoditized security products, but the real costs of concern are related to switching to new quantum safe technologies.

Quantum safe communication techniques are not compatible with techniques incumbent in products vulnerable to quantum attacks. In a well-ordered and cost efficient technology transition, there is a period of time where the new products are gradually phased in and legacy products are phased out.

# CHAPTER 2

## 2.1 INTRODUCTION

Cryptography is the problem of doing communication or computation involving two or more parties who may not trust one another. The best known cryptographic problem is the transmission of secret messages. Suppose wish to communicate in secret. For example, you may wish to give your credit card number to a merchant in exchange for goods, hopefully without any malevolent third party intercepting your credit card number. The way this is done is to use a cryptographic protocol. The most important distinction is between private key cryptosystems and public key cryptosystems.

The way a private key cryptosystem works is that two parties, 'Alice' and 'Bob', wish to communicate by sharing a private key, which only they know. The exact form of the key doesn't matter at this point – think of a string of zeroes and ones. The point is that this key is used by Alice to encrypt the information she wishes to send to Bob. After Alice encrypts she sends the encrypted information to Bob, who must now recover the original information. Exactly how Alice encrypts the message depends upon the private key, so that to recover the original message Bob needs to know the private key, in order to undo the transformation Alice applied.

Unfortunately, private key cryptosystems have some severe problems in many contexts. The most basic problem is how to distribute the keys? In many ways, the key distribution problem is just as difficult as the original problem of communicating in private – a malevolent third party may be eavesdropping on the key distribution, and then use the intercepted key to decrypt some of the message transmission.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that Alice and Bob's security cannot be compromised. This procedure is known as **quantum cryptography** or **quantum key distribution** (abbreviated QKD). The basic idea is to exploit the quantum mechanical principle that observation in general disturbs the system being observed. Thus, if there is an eavesdropper listening in as Alice and Bob attempt to

transmit their key, the presence of the eavesdropper will be visible as a disturbance of the communications channel Alice and Bob are using to establish the key. Alice and Bob can then throw out the key bits established while the eavesdropper was listening in, and start over.

## 2.2 LITERATURE SURVEY

Until fairly recently, the Information and Communication Technology (ICT) industry has considered information interchange transactions across electronic networks to be secure when encrypted using what are considered to be an unbroken conventional cryptographic system. Recent research in the field of quantum computing has produced a credible and serious threat to this assumption. Some problems that are considered difficult or impossible to solve using conventional computation platforms become fairly trivial for a quantum computer. Any information that has been encrypted, or will be encrypted using many of the industry's state-of-the-art cryptosystems based on computational hardness is now under threat of both eavesdropping and attack by future adversaries who have access to quantum computation.

This means that even encrypted information sitting in a database for 25 years for example, will be subject to discovery by those with access to quantum computing platforms. The discovery of the content of such data could lead to very serious consequences. These include the misuse of bank account numbers, identity information, items relating to military security and other sensitive information. Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure.

## 2.3 METHODOLOGIES

## 2.3.1 DESCRIPTION

1. **Cryptography**
2. **Types of Cryptography**

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Function

3. **Steganography**

1. Cryptography

Cryptography is literally the art of "secret writing". It is used to secure communication by protecting the confidentiality and integrity of messages and sensitive data. Without it, anyone could read a message or forge a private conversation. Messages are made secret by transforming them from "plaintext" into "cipher text" using a cipher and performing the process of encryption. Decryption turns scrambled and unreadable cipher text back into plaintext. When cryptographers talk about a "key", they are referring to a shared secret that controls the ability to hide and un-hide information. There are two types of cryptography that are often referred to as "symmetric key" and "public key" cryptography.

2. Types of Cryptography

- Symmetric Key Cryptography

In symmetric key cryptography, the same key is used for both encryption and decryption, and that key needs to be kept a secret by everyone who is sending and receiving private messages. The major difficulty of symmetric key cryptography is to provide the secret keys to legitimate parties without divulging the keys to eavesdroppers.

Asymmetric key cryptography

Asymmetric cryptography is often used to exchange the secret key to prepare for using symmetric cryptography to encrypt data. In the case of a key exchange, one party creates the secret key and encrypts it with the public key of the recipient. The recipient would then decrypt it with their private key. The remaining communication would be done with the secret key being the encryption key. Asymmetric encryption is used in key exchange, email security, Web security, and other encryption systems that require key exchange over the public network.

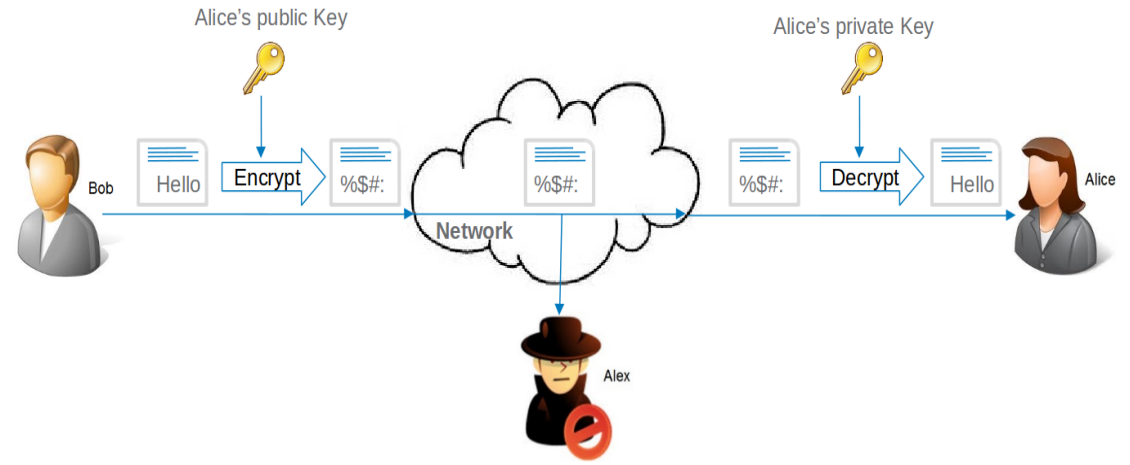
Hash function

A cryptographic hash function (CHF) is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest"). It is a one-way function, that is, a function which is practically infeasible to invert or reverse the computation. Ideally, the only way to find a message that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Cryptographic hash functions are a basic tool of modern cryptography.

3. Steganography

Steganography is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words steganós meaning "covered or concealed", and graphia meaning "writing".

## 2.3.2 SYSTEM DESIGN




Bob wants to send a private message to Alice, and the only easy way they have to communicate is via postal mail. Unfortunately, Bob is pretty sure that the postman is reading the mail she sends. That makes Bob sad, so she decides to find a way to send messages to Alice without anyone else being able to read them.

**Symmetric-KeyEncryption**

Bob decides to put the message inside a lockbox, then mail the box to Alice. She buys a lockbox and two identical keys to open it. But then she realizes she can't send the key to open the box to Alice via mail, as the mailman might open that package and take a copy of the key.

Instead, Bob arranges to meet Alice at a nearby bar to give him one of the keys. It's inconvenient, But she only has to do it once, After Bob gets home she uses her key to lock her message into the lockbox. Then she sends the lockbox to Alice. The mailman could look at the outside, or even throw the box away so Alice doesn't get the message – but there's no way he can read the message, as he has no way of opening the lockbox. Alice can use his identical key to unlock the lockbox and read the message. This works well , and now that Bob and Alice have identical keys Alice can use the same method to securely reply. Meeting at a bar to exchange keys is inconvenient, though. It gets even more inconvenient when Alice and Bob are on opposite sides of an ocean.

**Public-Key Encryption**

This time, Bob and Alice don't ever need to meet. First Alice buys a padlock and matching key.

Then Alice mails the (unlocked) padlock to Bob, keeping the key safe.

Bob buys a simple lockbox that closes with a padlock, and puts her message in it.

Then she locks it with Alice's padlock, and mails it to Alice. She knows that the mailman can't read the message, as he has no way of opening the padlock. When Alice receives the lockbox he can open it with his key, and read the message.

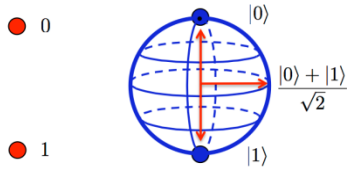
This only works to send messages in one direction, but Bob could buy a blue padlock and key and mail the padlock to Alice so that he can reply.

Or, instead of sending a message in the padlock-secured lockbox, Bob could send Alice one of a pair of identical keys.

Then Bob and Alice can send messages back and forth in their symmetric-key lockbox, as they did in the first example.

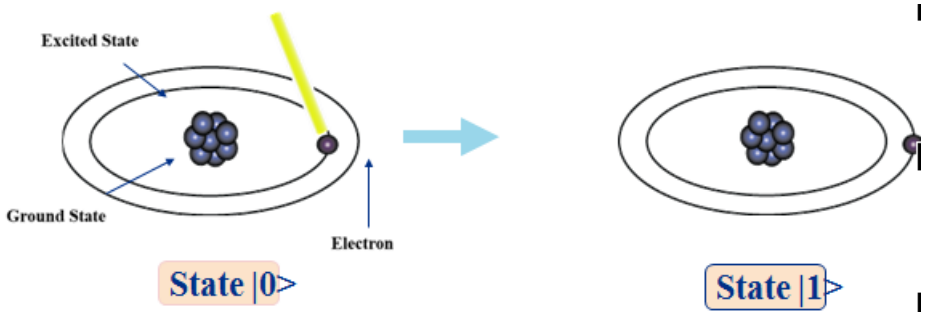
## 2.3.3 Representation of Data-Qubits

**Qubits**: the quantum version of classical bits. They are realized by a two-state device i.e. spin up and spin down, or the vertical and horizontal polarization of a single photon, or ground and excited states.



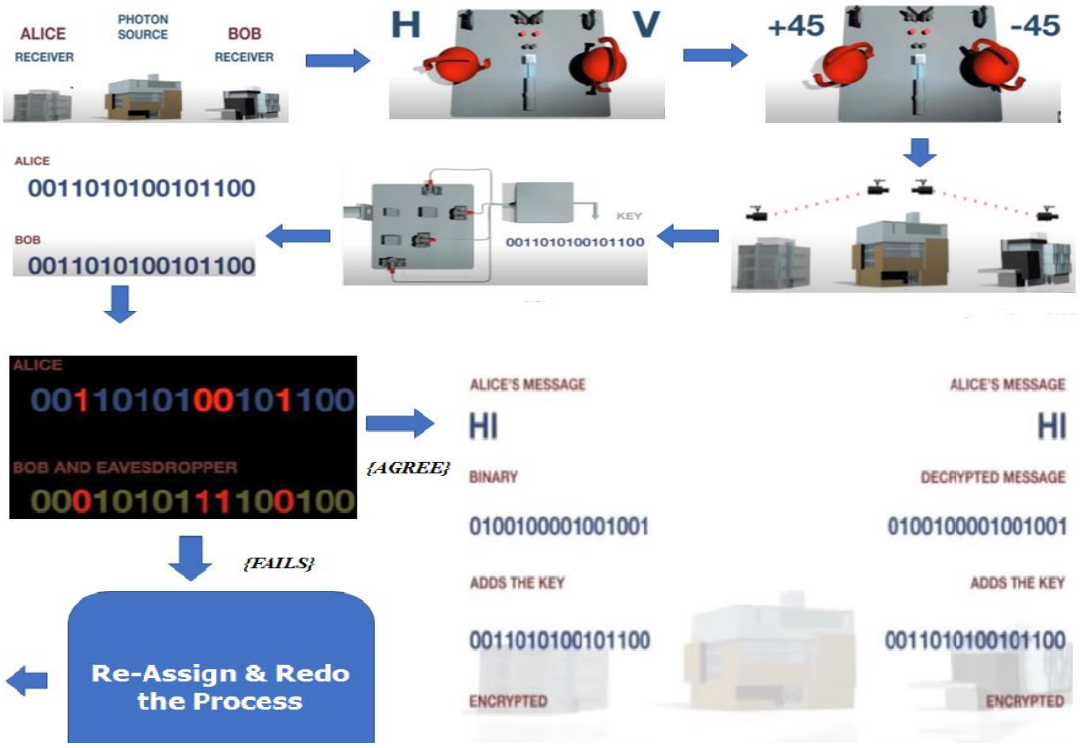

**Classical Bit** **Qubit**

- This allows for superposition and interference to happen, providing enormous computational power.
- A physical implementation of a qubit could use the two energy levels of an atom. An excited state representing |1> and a ground state representing |0>.



### 2.3.4 Quantum key distribution (QKD)

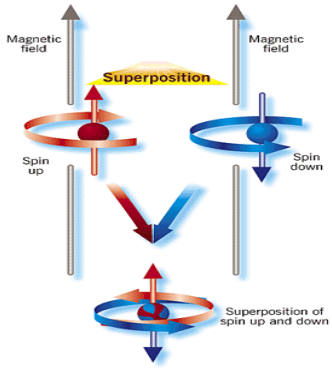
It is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.




### 2.3.5 Principles Of Quantum Cryptography

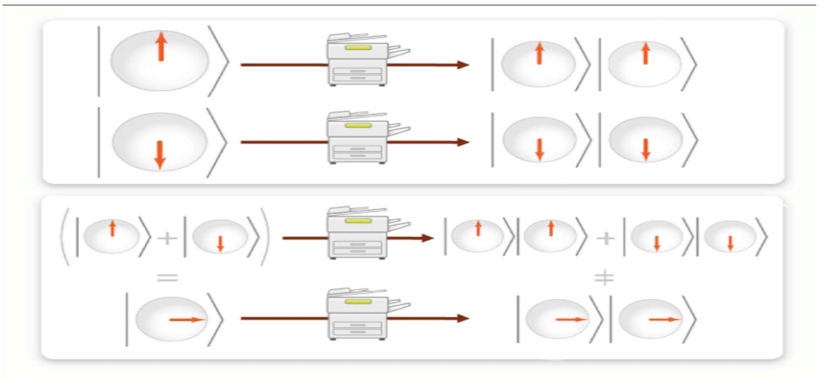
Quantum Superposition:

The qubit state can occupies all the states between 0 and 1 simultaneously, but collapses into 0 or 1 when observed physically. A qubit can therefore encode an infinite amount of information, but most of this information is useless as it can never be observed.



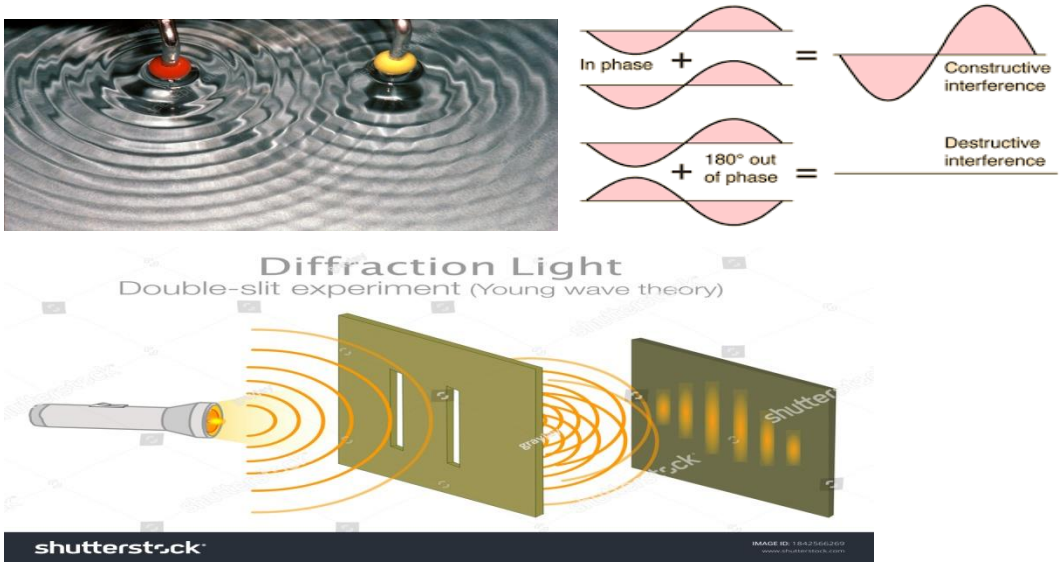

No- cloning theorem

The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state, a statement which has profound implications in the field of quantum computing among others.

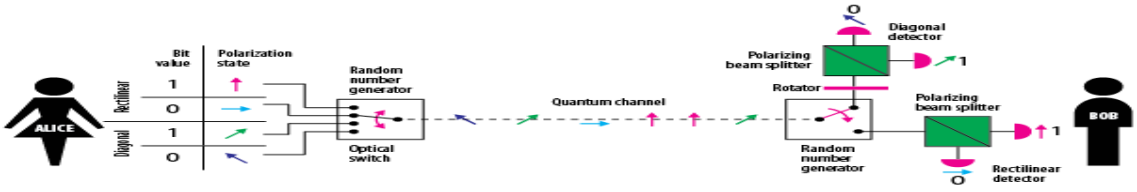


Quantum Interference:

Essentially, the concept states that elementary particles can not only be in more than one place at any given time (through superposition), but that an individual particle, such as a photon (light particles) can cross its own trajectory and interfere with the direction of its path.




BB84 protocol




| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Quantum transmission & detection | ALICE sends photons | ↖ | ↗ | → | ↑ | ↑ | ↗ | ↖ | ↑ |
| | ALICE's random bits | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| | BOB's detection events | ↑ | ↗ | ↖ | ↑ | ↗ | ↗ | ↖ | ↖ |
| | BOB's detected bit values | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| Public discussion (i.e., sifting) | BOB tells ALICE the basis choices he made | + Rect | × Diag | × Diag | + Rect | × Diag | × Diag | × Diag | × Diag |
| | ALICE tells BOB which bits to keep | | ✓ | | ✓ | | ✓ | ✓ | |
| | ALICE and BOB's shared sifted key | – | 1 | – | 1 | – | 1 | 0 | – |

# CHAPTER 3

## 3.1 SYSTEM DESIGN

## 3.2 Softwares

- **Qiskit**

  An open-source software development kit to prepare, run, and measure quantum states on IBM's quantum computers. The used model of computation is quantum circuits, where quantum algorithms consist of consecutive gates.

- **QuTip**

  An open-source Python-based software for simulating the dynamics of noisy quantum systems

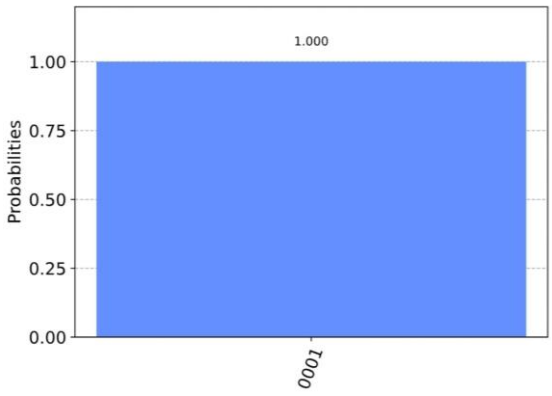
- **Streamlit Api**

- **Python**
- **Julia notebook**

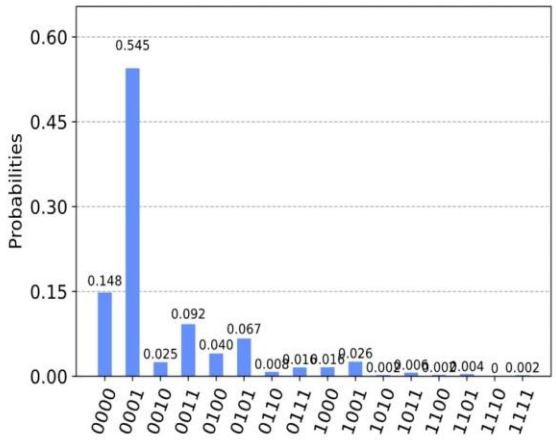
Simulation done on 3 different hardware platforms

- **SIMULATOR**

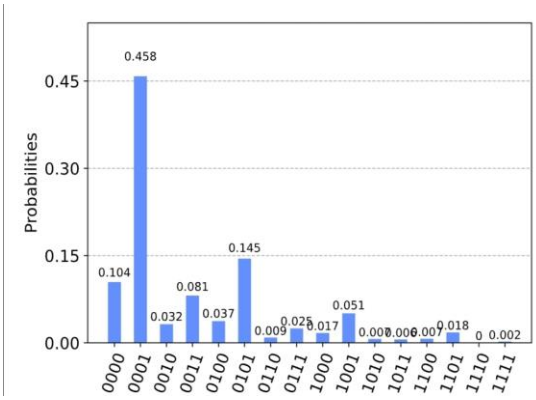
  Simulator software is based on the process of modeling a real phenomenon with a set of mathematical formulas. It is, essentially, a program that allows the user to observe an operation through simulation without actually performing that operation. Simulation software is used widely to design equipment so that the final product will be as close to design specs as possible without expensive in process modification. Simulation software with real-time response is often used in gaming, but it also has important industrial applications. When the penalty for improper operation is costly, such as airplane pilots, nuclear power plant operators, or chemical plant operators, a mock up of the actual control panel is connected to a real-time simulation of the physical response, giving valuable training experience without fear of a disastrous outcome.



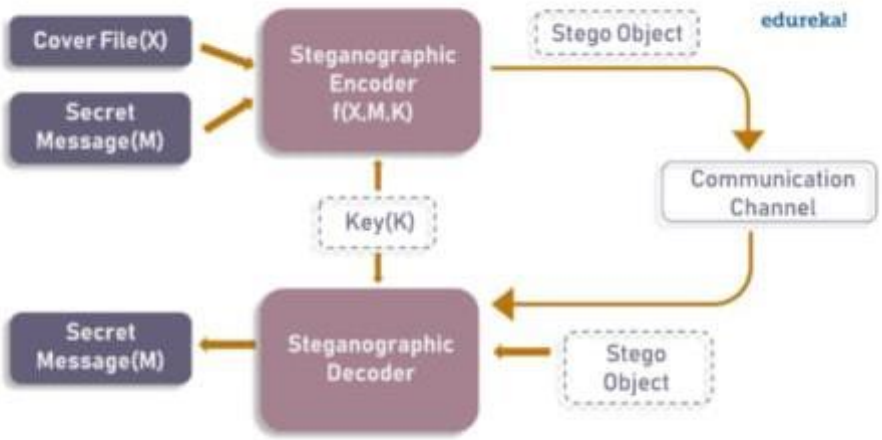

- **IBMQ-BOGOTA**




- **HYBRID**



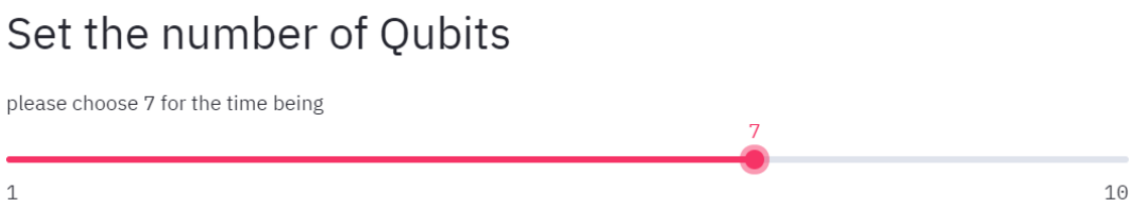
## 3.2.1 Project Description and Implementation results




The encoder circuit is based on 7 qubits but our interactive application has an option to create circuits based on the number of qubits selected and view them instantaneously.

Here are some steps to interactively play with our application:

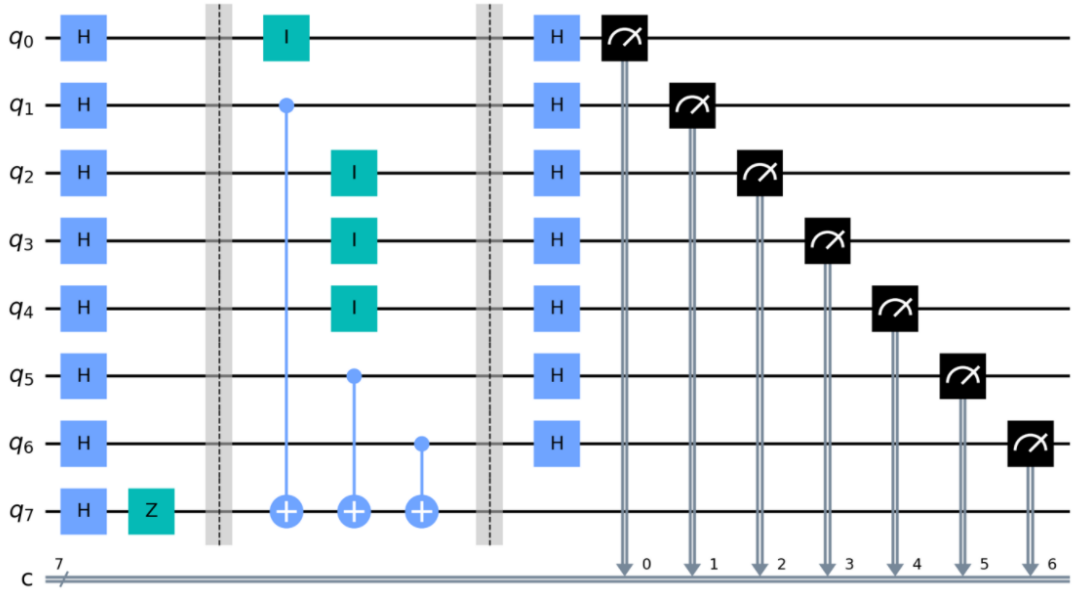
- Choose the number of qubits using the slider. We would suggest that you choose 7 for the encoding and decoding scheme to work flawlessly you can also test out other number of qubits to view the generated circuit. The idea is to encode the sender's text (secret message) using the concept of interference. The secret message is encoded based on the cover file (a text sentence in this case). We have chosen our cover file and the secret message to be in text formats to make it easier for new learners to understand the concept of quantum steganography while also trying it out interactively in a console.



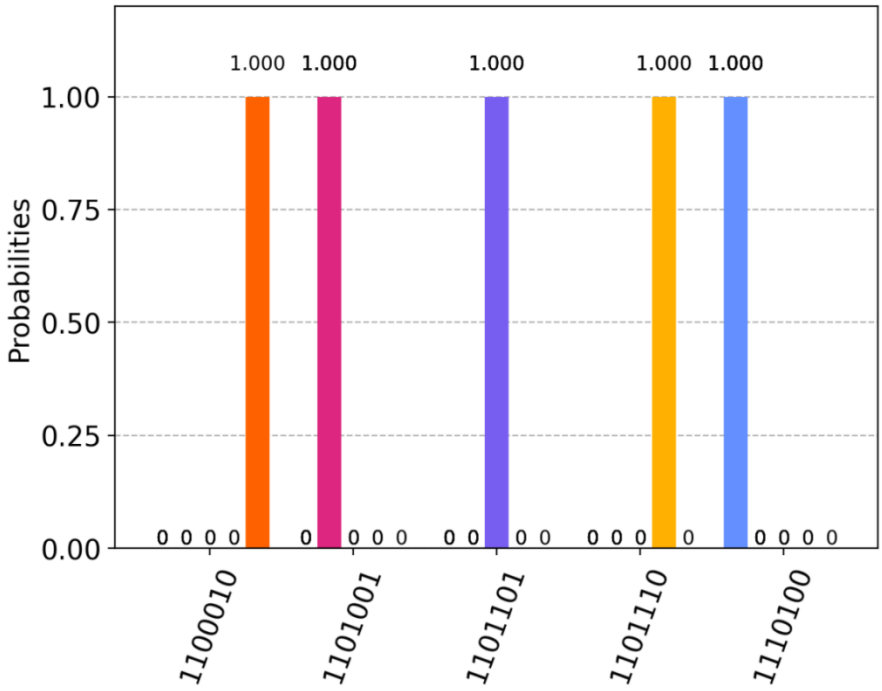
- Enter the Secret message and press enter. You could try out qiskit as one of the test words.

## Secret Message:

bnmit




Here, you can also view the generated circuit.

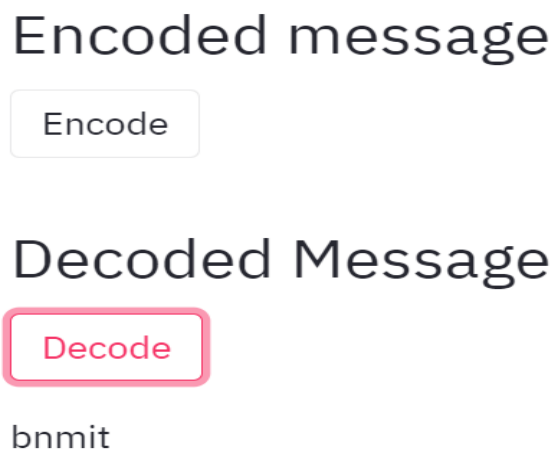


The obtained outcome of the circuit is show in graph

Upload a sentence where you wish to hide your message and press enter. You could try this sentence:

hellooo bangalore hellooo bangalore hellooo bangalore

Click of encode to view the encoded message and then click on decode to finally view your original message.



5469 lines (5469 sloc) | 234 KB

In [1]:
```
import qiskit
from qiskit import *
import numpy as np
import matplotlib.pyplot as plt
from qiskit.visualization import plot_histogram
```

Create the quantum circuit for the BB84_keys:

In [2]:
```
# Creating registers with n qubits
n =7  # for a local backend n can go as up as 2
3, after that it raises a Memory Error
qr = QuantumRegister(n, name='qr')
cr = ClassicalRegister(n, name='cr')

qc = QuantumCircuit(qr, cr, name='QC')
```

QRNG

BB84 Protocol :

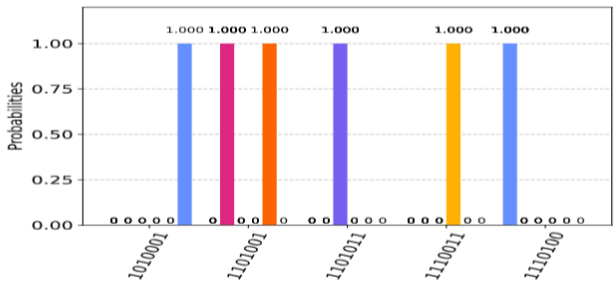
In [6]:
```
# Generate a random number in the range of avail
able qubits [0,65536))
alice_key = np.random.randint(0,2**n)#here we ca
n remplace by a key from a quantum key generator


alice_key = np.binary_repr(alice_key,n)
```

In [7]:
```
print(alice_key)
```

0001110

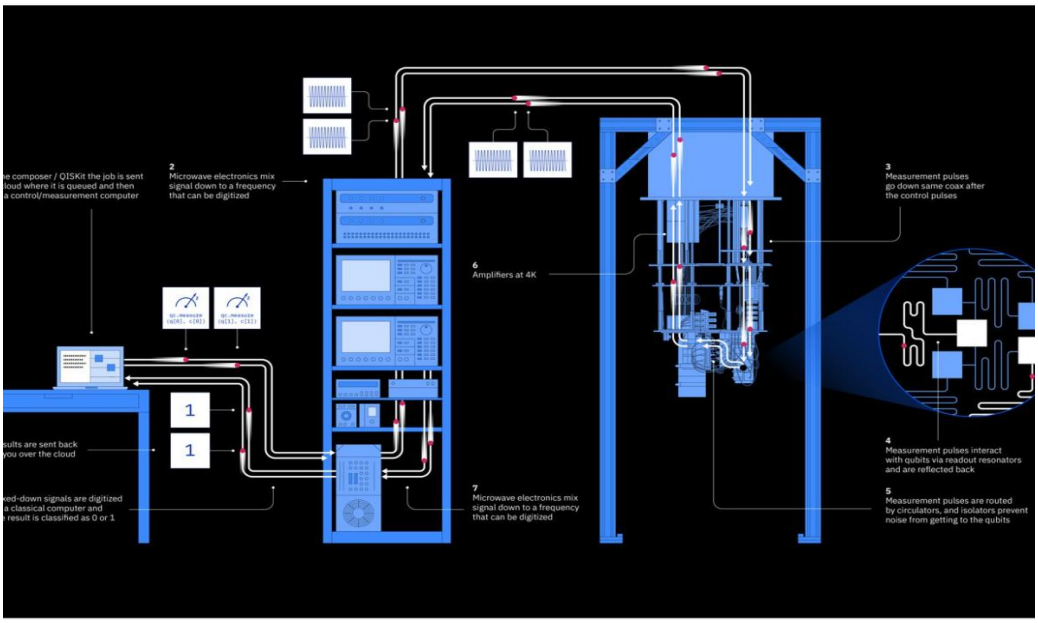
```
results = execute(circuit_to_run[::-1], backend=
backend, shots=shots).result()
answer = results.get_counts()

plot_histogram(answer)
```

Out[18]:

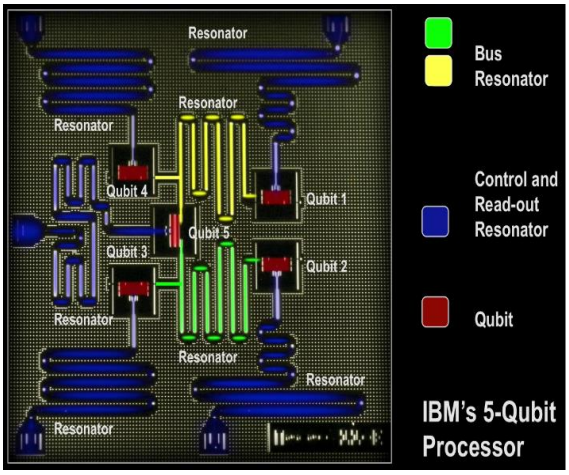


## 3.2.2 Hardware

### IBM QUANTUM CLOUD ARCHIETECTUTE

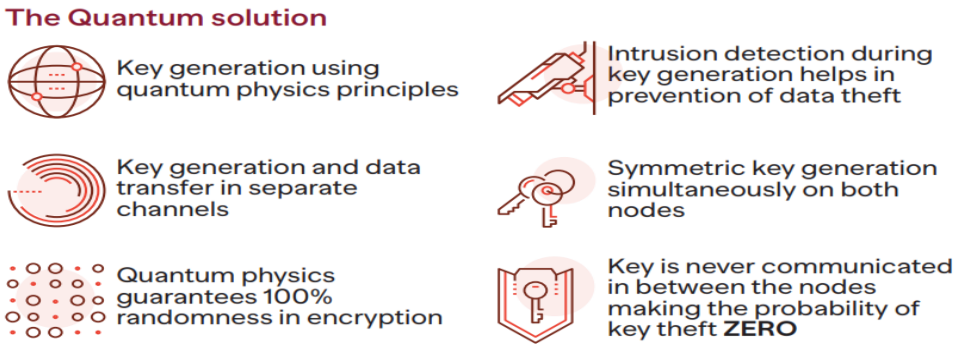



### IBM's 5 QUBIT PROCESSOR




## 3.2.3 Making encryption quantum-safe

Conventional methods will not help in building quantum-safe cryptography. Here, quantum physics equips us not only with the required principles to battle with future quantum computers, but also equips us to make the whole crypto-system unbreakable. Quantum physics by its very nature is very different from classical physics. Using these new laws, the keys in cryptography attain perfection with unconditional security. The advantages are mentioned below.




## 3.2.4 Inducement and Future Development

• The potential benefits of quantum computing, from advances in cancer research, gene-studies to unlocking the mysteries of the universe, are limitless. But that same computing power can be used to unlock different kinds of secrets—from one's personal finances, health records, to corporate research projects and classified government intelligence.

• The greatest impact of quantum revolution will be felt on cryptography. A sufficiently large quantum computer running the existing Shor's algorithm can crack RSA or Diffie Hellman system of encoding in seconds as opposed to millions of years by brute force method today.

• Symmetric key systems such as AES, 3DES etc. which are used for end to end bulk encryptors are more resilient, however, even these can be cracked in relatively quicker time frames by running the Grover's algorithm on a quantum computer. Even these systems use Diffie Hellman for key exchange which will become completely insecure.

• The only solution is to evolve a new breed of Post Quantum cryptographic systems resilient to algorithmic simulations. Another aspect to note, no matter the encryption system used its security is limited by the security of its key.

• In order to understand the graveness of the threat, imagine the security systems that protect a company's information in the form of a pyramid, from the least secure to the most secure protection Quantum factor at the base will be a major threat, but there are many factors above, which will cater to security for any company.

# CHAPTER 4

## 4.1 CONCLUSION AND RECOMMANDATION

## 4.2 CONCLUSION

- Quantum cryptography is a major achievement in security engineering.
- As it gets implemented, it will allow perfectly secure bank transactions, secret discussions for government officials, and well-guarded trade secrets for industry.
- Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology.
- The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved.
- Quantum computing indeed poses a credible threat to conventional information security systems. The ICT community nevertheless has the ability to analyse and better understand this threat and its consequences for the various categories of information that requires protection.

## 4.3 RECOMMENDATION

There are a number of short-term precautionary measures that can mitigate this problem. While the US cannot take back any encrypted data already in the possession of adversary intelligence agencies, the US can institute a number of short-term reforms that can make the impact of this reality less of a security issue by stemming the flow of future data to adversaries.

# REFERENCES


1. Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data, Dr.Takashi Mihara, Future Creation Laboratory, Olympus Corporation.
2. Quantum cryptography: An emerging technology in network security, Mehrdad S. Sharbaf, Marymount University, California state University
3. Quantum Cryptography and Quantum Key Distribution Protocols: A Survey, V.Padmavathi, B.Vishnu Vardhan, A.V.N Krishna
4. Qiskit 0.25.4 documentation, IBM Quantum Community
5. C. H. Bennett, G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing.