QUANTUM COMPUTING AND ITS APPLICATIONS

Soumyadeep Das
AP20110010181
CSE – "C"

M. Aishwary
AP2011001209
CSE – "C"

Akash Kumar
AP20110010150
CSE – "C"

Utkarsh Majumdar
AP20110010205
CSE – "C"

Vishnu Vardhan
AP20110010199
CSE – "C"

Abstract— **Quantum computing is a global race to conceive and create the ultimate computing machine. Can u think of a computer whose memory is larger than its apparent physical size? Or a computer that can manipulate an exponential set of inputs simultaneously? The answer to this question is also an answer to a much big problem to be faced in the future-** ***THE CONCEPT OF QUANTUM COMPUTERS.*** **A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behaviour of particles at the sub-atomic level. Quantum computers open up a new era for high-speed computation. They will be 1,000,000,000 times faster than the current silicon-based computers. Quantum computers will be able to rapidly factor extremely large numbers, making them extremely useful for solving certain large mathematical problems at speeds faster than today's fastest supercomputers and for cracking secret codes that have been encrypted by traditional methods. A functional quantum computer would put much of the world's past and present encrypted information at risk of being quickly deciphered. This paper deals with the basic concepts of quantum computing and its impact in cryptography.**

I. INTRODUCTION

"A PROBLEM IS THE MOTHER OF ALL INVENTIONS ". This statement holds true in the case of Quantum computers also. Apart from man's urge for supercomputers, it is the problem as predicted by Gordon Moore, co-founder of Intel that gave rise to the all-new emerging and active branch in computers-"Quantum Computers". The idea of Quantum computers originated in 1980 when P. Benioff thought about the Turing machine. Shor's algorithm is the first significant problem solved by a quantum approach to excel classical computers.

Scientists already think about a quantum computer, as a next generation of classical computers. Gershenfeld says that if making transistors smaller and smaller is continued with the same rate as in the past years, then by the year of 2020, the width of a wire in a computer chip will be no more than a size of a single atom. These are sizes for which rules of classical physics no longer apply. Computers designed on today's chip technology will not continue to get cheaper and better. Because of its great power, quantum computers are an attractive next step in computer technology. Around 2030 computers might not have any transistors and chips. Theoretically it can run without energy consumption and is a billion times faster than today's PIII computers.

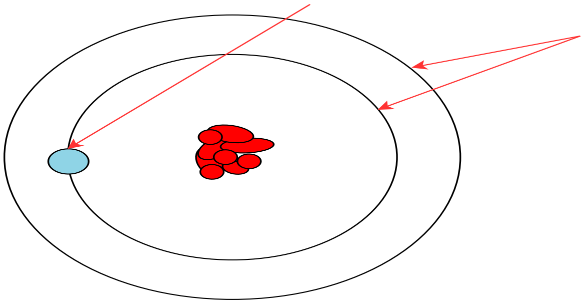
The technology of quantum computers is also very different. For operation, quantum computers use quantum bits (qubits). Qubits have a quaternary nature. A qubit can exist not only in the states corresponding to the logical values 0 or 1 as in the case of a classical bit, but also in a superposition state. A qubit is a bit of information that can be both zero and one simultaneously (Superposition state). Thus, a computer working on a qubit rather than a standard bit can make calculations using both values simultaneously. A qubyte is made up of eight qubits and can have all values from zero to 255 simultaneously. "Multi-qubyte systems have a power beyond anything possible with classical computers. Massachusetts Institute of Technology, Oxford University, IBM and Los Alamos National Laboratory are the most successful in the development of quantum computers.

A. Features

- 300 qubits can store more than 10^90 numbers simultaneously. That's more than the number of atoms in the visible universe! This shows the power of quantum computers.
- Integer factorization is believed to be computationally feasible with a quantum computer for large integers that are the product of only a few prime numbers (e.g., products of two 300-digit primes)
- Quantum computers are reversible, and therefore there is theoretically no net energy consumption.
- A quantum computer can simulate physical processes of quantum effects in real time.
- Forty qubits could have the same power as modern supercomputers. According to Chuang, a supercomputer needs about a month to find a phone number from the database consisting of the world's phone books, where a quantum computer is able to solve this task in 27 minutes. Encryption technology is a mere possibility with the help of quantum computers.
- Super dense communication and Ultra secure communication is one of the very useful applications of quantum computers.

B. Bits And Qubits

The basic data unit of a conventional computer is the bit. A bit stores a numerical value of either '0' or '1'. We could also represent a bit using two different electron orbits in a single atom. In most atoms, there are many electrons in many orbits. But we need to consider only the orbits available to a single outermost electron in each atom.



However, a completely new possibility opens up for atoms. Electrons have a wave property that allows a single electron to be in two in orbits simultaneously. In other words, the electron can be in superposition of both orbits.

Electron in both orbits simultaneously

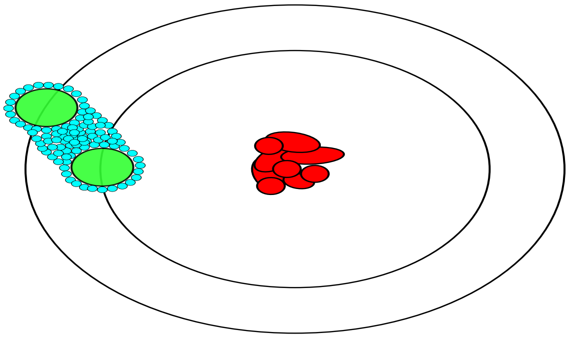


Fig: Concept of a Qubit.

To distinguish this new kind of data storage, it is called quantum bit 0r qubit. The key point is that a qubit can be in a superposition of the digits ‘0’ and ‘1’. Superposition states allow many computations to be performed simultaneously, and give rise to what is known as Quantum parallelism.

C. Definition Of Qubit

Consider an atom with at least two discrete and sufficiently separated energy levels. In an atom, the energy levels of the various electrons are discrete; two of them can be selected and labelled as logical 0 and 1.

Consider an atom with only one electron and two energy levels, a ground state (0) and an excited state(1). By using a light pulse of half the duration as the one needed to perform the NOT operation, we effect a half- flip between the two logical states. It means that the state of the atom after the half pulse is neither 0 nor 1 but a coherent quantum superposition of both states. This is called a QUBIT and it stores both 0 and 1 simultaneously.

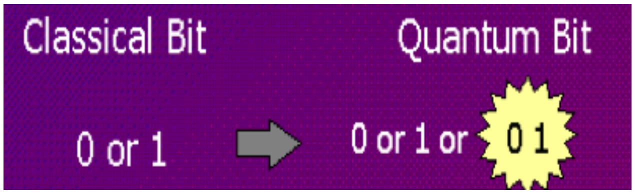
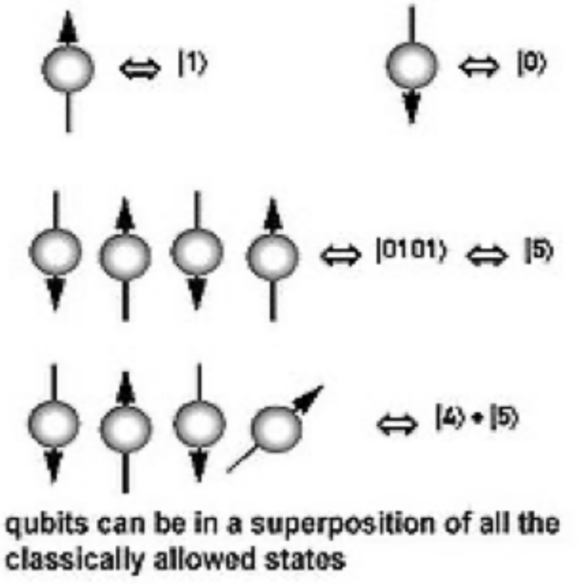


Fig: Classical bit v/s Qubit.



qubits can be in a superposition of all the classically allowed states

Using this kind of “half—pulses”, it is possible to create super positions of states in the memory of quantum computers, opening new ways to perform computations.

D. Quantum Registers

Now we push the idea of superposition of numbers a bit further. Consider a register composed of three physical bits. Any classical register of that type can store in a given moment of time only one out of eight different numbers i.e. the register can be in only one out of eight possible configurations such as 000, 001, 010, ... 111. A quantum register composed of three qubits can store in a given moment of time all eight numbers in a quantum superposition. This is quite remarkable that all eight numbers are physically present in the register but it should be no more surprising than a qubit being both in state 0 and 1 at the same time.

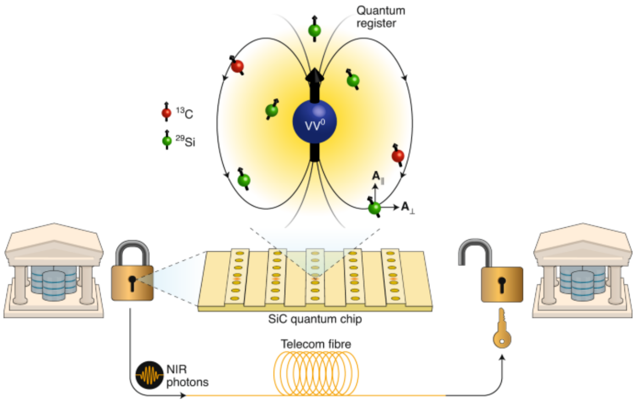


Fig: Quantum Register.

E. Superpositioning

Superpositioning means that two things overlap without interfering with each other. In classical computers, electrons cannot occupy the same space at the same time, but in the case of a qubit the electron acts as a wave and thus it can. The waves can also be superimposed and also, they can be retrieved from one another by subtracting the other.

By the concept of superpositioning the electron can thus occur at two orbits in an atom simultaneously and thus can represent two digits simultaneously.

F. Quantum Parallelism

A one bit can store one of the digits ‘0’ and ‘1’. Likewise, a two-bit memory can store one of the binary numbers ‘00’, ‘01’, ‘10’ and ‘11’. But these memories can store only a single number at a time. In contrast, a quantum superposition state allows a qubit to store ‘0’ and ‘1’ simultaneously. Two qubits can store all the four binary numbers. The table below gives a much better view of the power of a qubit.

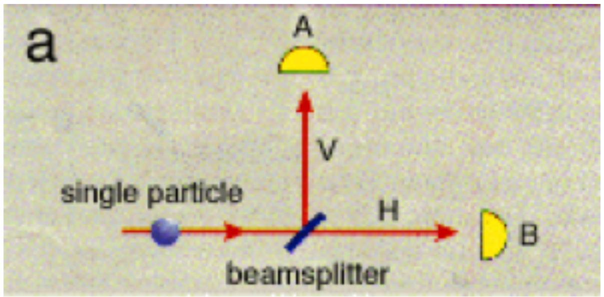
Numbers Stored by Qubits:

Qubits	Stores simultaneously	Total number
1	(0 and 1)	2! = 2
2	(0 and 1)(0 and 1)	2*2 = 4
3	(0 and 1)(0 and 1)(0 and 1)	2*2*2 = 8
:	: :	:
300	(0 and 1)..(0 and 1)	2*2……..*2 = 2^300

The table shows that 300 qubits can store more than 10^90 numbers simultaneously. That’s more than the number of atoms in the visible universe! This shows the power of quantum computers.

G. Quantum Interference

The concept of Quantum interference can be explained with the famous Single particle interference effect. This says that whenever a photon is passed through a half-silvered mirror it splits and the probability that the photon travels in both directions is equal. This means that the photon travels in both the directions simultaneously.



H. Entanglement And Quantum Teleportation

When two quantum systems are created while conserving some property, their state vectors are correlated, or entangled. For example, when two photons are created, and their spin conserved, as it must, one photon has a spin of '1' and '-1'. By measuring one of the state vectors of the photon, the state vector collapses into a knowable state. Instantaneously and automatically, the state vector of the other photon collapses into the other knowable state. There are no forces involved and no explanation of the mechanism.

The principle of entanglement enables a phenomenon called 'Quantum teleportation'; it involves the destruction of the original and recreation of an exact replica at another location.

I. Applications and The Power of Quantum Computers

1. Encryption technology
2. Ultra-secure and super dense communication
3. Improved error correction and error detection
4. Molecular simulations
5. True Randomness
6. Artificial Intelligence

J. Some Problems in Production of Quantum Computers

- Decoherence - It is that quantum computation will spread outside the computational unit and will irreversibly dissipate useful information to the environment.
- Error Correction – Error correction is rather self-explanatory, but what errors need correction? The answer is primarily those errors that arise as a direct result of decoherence
- Hardware architecture

K. Quantum computing can efficiently break

- RSA
- Diffie-Hellman key exchange
- Elliptic curve cryptographic system

Quantum computers will soon allow the cracking of every cipher. Quantum encryption will soon provide unbreakable ciphers. Does something sound contradictory about those statements? The fact is we have a bit of a dichotomy here, and with teams on both sides of the argument fervently pushing their contradictory visions it can be hard for computer security professionals to separate the fact from the hype.

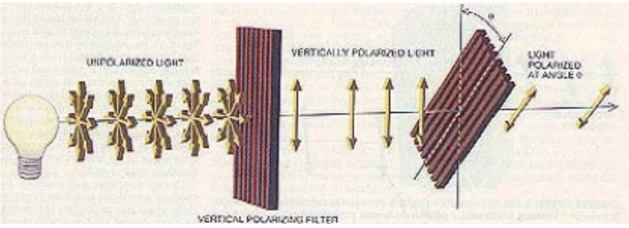
L. Quantum Cryptography

Quantum Cryptography or Quantum Encryption is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic keys using the transmission of quantum states of light. The security of these transmissions is based on the laws of quantum mechanics and theoretically secure pre and post transmission processing methods.

1. *Why quantum cryptography?*
   - Protect against attack by quantum computer or any future machine.
   - Eavesdropping detection.
   - High volume key distribution if it can be made fast enough.

Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. The word quantum itself refers to the most fundamental behavior of the smallest particles of matter and energy: quantum theory explains everything that exists and nothing can be in violation of it.

Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model. Essentially, quantum cryptography is based on the usage of individual particles/waves of light (photon) and their intrinsic quantum properties to develop an unbreakable cryptosystem - essentially because it is impossible to measure the quantum state of any system without disturbing that system. It is theoretically possible that other particles could be used, but photons offer all the necessary qualities needed, their behavior is comparatively well-understood, and they are the information carriers in optical fiber cables, the most promising medium for extremely high-bandwidth communications.


UNPOLARIZED LIGHT
VERTICALLY POLARIZED LIGHT
LIGHT POLARIZED AT ANGLE Θ
Θ
VERTICAL POLARIZING FILTER

Thus, quantum cryptography is a way to combine the relative ease and convenience of key exchange in public key cryptography with the ultimate security of a one-time pad.

2. *How It Works in Practice?*

In practice, quantum cryptography has been demonstrated in the laboratory by IBM and others, but over relatively short distances. Recently, over longer distances, fiber optic cables with incredibly pure optic properties have successfully transmitted photon bits up to 60 kilometers. For information security, it means that any trial of eavesdropping or interception of the transmission realized with the help of elementary particles would be instantly detected. The domain, in which quantum cryptography evokes the greatest hopes, is safe exchange of coding keys between sites which participate in communication.

Practical applications in the US are suspected to include a dedicated line between the White House and Pentagon in Washington, and some links between key military sites and major defense contractors and research laboratories in close proximity.

II. CONCLUSION

To conclude, we can state that quantum computation is not a distant dream because the last century witnessed a huge topsy-turvy regarding size of electronic circuits, from vacuum tubes to transistors , from transistors to wired logic to integrated circuits.

MOORE’S LAW: The density of transistors on a single chip doubles every 18 months.

Electronics and VLSI engineers have so far obeyed Moore’s law. If they are to continue validating this law, they have to devise newer methods for fabrication of circuits.

Some of the methods may be:

- Using other materials in addition to silicon.
- Using polymers in fabrication.
- New methods of computing like DNA Computing and Quantum Computing.

So, it can be concluded that quantum computing is set to create unprecedented growth in terms of memory and speed as far as computation is concerned.

Building a practical quantum computer is just a matter of time. Quantum computers easily solve applications that can’t be done with the help of today’s computers. This will be one of the biggest steps in science and will undoubtedly revolutionize the practical computing world.

III. ACKNOWLEDGEMENT

We are deeply grateful to all those who have contributed to this report. Our sincere thanks go to Dr. Manjula R for their invaluable guidance and support throughout the process.

We are also grateful to her for providing us with access to valuable data and resources. Their willingness to share their knowledge and experience was greatly appreciated.

Finally, we would like to express our gratitude to our colleagues and friends who offered their encouragement and support during the course of this paper. We could not have completed this work without their help and we are grateful for their contributions.

IV. REFERENCES

1. The Fabric of Reality. David Deutsch

2. Physics - A Textbook for Advanced Level Students. Tom Duncan

3. Algorithmics - The Spirit of Computing. David Harel

4. A quantum revolution for computing. Julian Brown, New Scientist 24/9/94

5. The best computer in all possible worlds. [Tim Folger]

6. Cue the qubits: https://www.cs.bgu.ac.il/~elhadad/summary-test/quant/text.html

7. Quantum keys for keeping secrets. Artur Ekert

8. Bulk Spin Resonance Quantum Computation https://pubmed.ncbi.nlm.nih.gov/8994025/