iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** XI **Month of publication:** November 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XI, Nov 2018- Available at www.ijraset.com

Quantum Information Processing

Mr. Himanshu Sharma
Assistant Professor, Department of Computer Science & Engineering, Translam Institute Of Technology & Management, Meerut, Uttar Pradesh, India

Abstract: ***Quantum Information Processing (QIP) is an active field in which quantum entanglement properties of superposition states are exploited to enhance and improve speed, versatility and performance of measuring quantum information and processing resulting instructions. QIP uses qubits as its basic information. QIP has many facts from quantum simulation, to cryptography, to quantum processing techniques, which is highly solve more complex problems than those with in the capabilities of conventional computers. Quantum Information Processing (QIP) is a high impact, experimental and theoretical research in all areas of Quantum Information Science (QIS). Quantum Information Science is an area of study based on the idea that information science depends on quantum effect in physics. Quantum Physics has to be considerd for device operation. Technologies based on quantum physics could improve the clock speed of microprocessors, decrease power dissipation and miniaturize more. It include quantum encryption, decryption and communication, quantum algorithms, quantum computer science, quantum image processing and sensing. Interest in quantum technologies and fabrication of trustable devices that exploit quantum mechanism is growing with computing, information processing and sensing. The aim of this collection is to capture the latest advances in solid- state systems for quantum information processing (QIP) and quantum communication. The spotlight collection aims to publish paper at forefront of nanoscale science and technology that impact the field of quantum information processing (QIP), either in the short or long term. The spotlight is on meso and nano scale devices and structures that host, measures and control qubits or other quantum dots and wires, spin qubits (ions, molecular, magnets etc), superconducting qubits and superconductor, semiconductor hybrids, topological materials and nanophotonics. The scope of this collection also includes-***

1) Designing and fabrication of device
2) Performance and reliability of device
3) Nano scale materials and characterization

Keywords: QIP, QIS, Qubits, QKD, QIT

I. INTRODUCTION

Quantum Information Theory (QIT) is the study of how to integrate information with quantum mechanism by studying how information can be stored and retrieved from a quantum mechanical system. Quantum information theory is nothing but dealing with computers using quantum physics and hence its algorithm called quantum computing. Computation with coherent atomic scale dynamics is called quantum computation. The behaviour of a quantum computer is governed by the laws of quantum mechanics. In quantum systems possibilities count, even if they never happen, like particle theory. Each of exponentially many possibilities can be used to perform a part of a computation at the same time. Quantum computation is more powerful than classical computation.

II. QUANTUM COMPUTERS

A. Quantum computers are devices that can carry out computations using quantum mechanical properties such as superposition and entanglement.
B. Qubits, quantum bits, are used to described states similar to the bit in transistor-based computing.
C. Quantum computers offer not only an increase in speed over classical computers but allows us to solve problems such as factoring as a exponentially faster.
D. They require very controlled system to prevent decoherence of qubits, a process in which an they are interrupted by some output influence and collapse to their 0 or 1 state, losing all the superposition probabilities they once stored.
E. Study of information processing tasks can be accomplished using quantum mechanical system.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue XI, Nov 2018- Available at www.ijraset.com

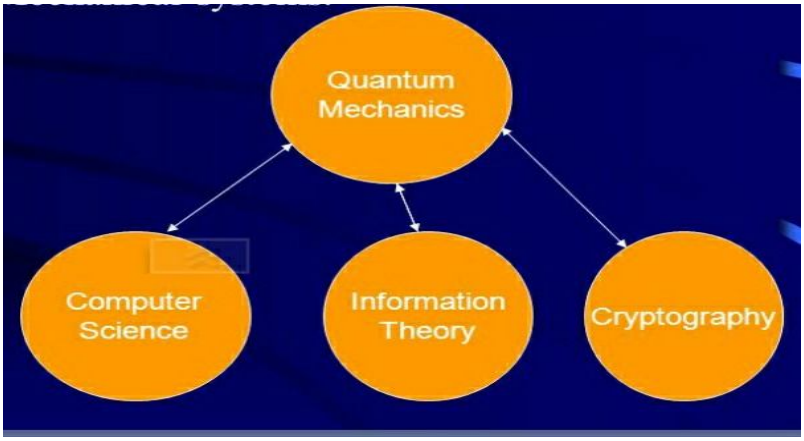


Fig.1. Quantum Mechanical System

III. QUBITS

A. Digital computers have bit.
B. Quantum computers have qubit.
C. The primary piece of information in quantum information processing is the qubit, an analog to the bit either 0 or 1 in classical information theory.
D. Qubit is also called quantum bit and it is the basic unit of quantum information.
E. The two position states of a photon in a Mach Zehnder apparatus is one of the example of a quantum bit or qubit.
F. They can be implemented using any quantum property that has two states and is observable, such as the spin of electrons.
G. Qubits can take advantage of quantum entanglement, where the states of two qubits depend on each other even though they may be at a distance, to perform operations on multiple data sets simultaneously
H. Qubits will "collapse" to a 0 or 1 state when measured.
I. Quantum gates can perform operations on qubits similar to transistor based gates performing logical operations such as AND on bits.

Particle theory is used in quantum systems possibilities which states that the particle can exist in a linear combination or superposition of two paths. This concept is applied here using qubits for computations. Any transformation on qubits can be done from composition of any two quantum gates, it is the statement of quantum computation theorem.

IV. QUANTUM GATES

A. Quantum Gates are similar to classical gates, but do not have a degenerate output. i.e. their original input state can be derived from their output state, uniquely. They must be reversible.
B. Quantum Gate is a basic quantum circuit which is operating on the small numbers of qubits.
C. This means that a deterministic computation can be performed on a quantum computer only if it is reversible.

V. QUANTUM PHYSICS CONCEPTS USED

The following quantum physics concepts are used in Quantum Information Processing-

A. Superposition: Superposition is a principle of quantum theory. The principle of superposition claims that while we don't know what the state of any object is, it is actually in all possible states simultaneously. Mathematically it refers to a property of solutions to the Schrodinger equation.
B. Interference: Interference is the phenomenon in which two waves superpose each other to form a resultant wave of greater or lower amplitude.
C. Coherence: Coherence is a property of waves that enables stationary that is temporally and constant, interference.
D. Entanglement: Entanglement is a term used in quantum theory to describe the way that particles of energy can become correlated to predictably interact with each other regardless of how far apart they are.

©IJRASET: All Rights are Reserved

VI. QUANTUM V/S CLASSICAL COMPUTERS

A. Quantum Computers

1) Quantum computers can use any particle which exhibits quantum properties to represent states called qubits.
2) Qubits can be a superposition of 0 and 1 states.
3) In order to get a reliable answer, algorithms must be carried out multiple times.
4) Fully functional quantum computers are still many years in the future.
5) Two slits experiment with electrons
6) Stern-Gerlach experiment

B. *Classical Computers*

1) Classical computer uses electrons to represent states called bits.
2) In these computers bits only handle a 0 or 1 state.
3) They giving very stable, expected answer for almost every operation with a high degree of accuracy.
4) Experiments with bullets and waves.
5) Practical using today's technology.

VII. SOME OF THE DIFFICULTIES WITH QUANTUM COMPUTING

1) *Decoherence*: the tendency of a quantum computer to decay from a given quantum state into an incoherent state as it interacts or entangles with the state of the environment
2) *Error Correction*: the answers that the operations are only right a percentage of the time using current quantum technologies
3) Hardware architecture

VIII. QUANTUM INFORMATION PROCESSING

A. Quantum Cryptography.

1) Public Key cryptography
2) RSA algorithm.

In computer science, quantum information is information that is held in the state of a quantum system.QIP is the basis entity of study in quantum information theory, and can be manipulated using engineering techniques known as quantum information processing.

B. Cryptography Operation

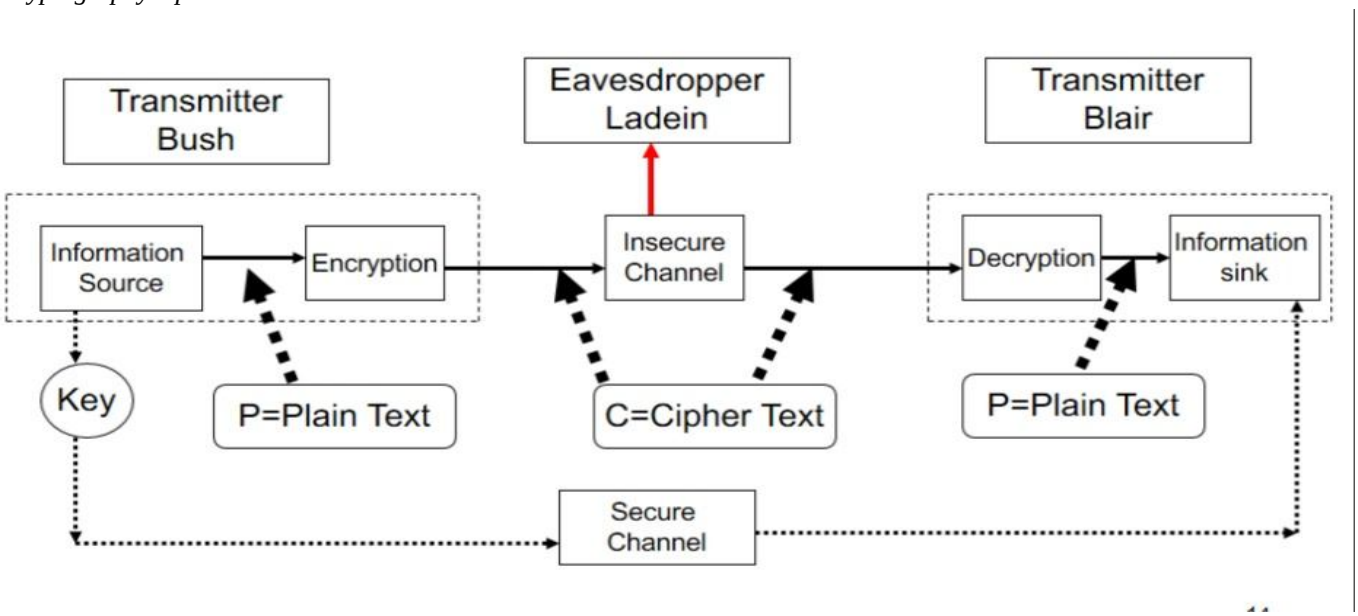


Fig.5. A Classical Cryptographic Communication System

©IJRASET: All Rights are Reserved

C. The RSA Algorithm

RSA (Rivest Shamir Adleman) develop this public key cryptography algorithm

1) ALGO

a) Select two primes p and q
b) Calculate n = p q
c) Calculate f(n) = (p-1)(q-1)
d) Select e such that 1 < e < f(n) and gcd(f(n),e) = 1
e) Calculate d = e^{-1} mod f(n)
f) Public key KU = {e,n}
g) Private key KR = {d,n}

2) Example

a) Select two primes p=7 and q=17
b) Calculate n = p q = 119
c) Calculate f(n) = (p-1)(q-1) = 96
d) Select e such that 1 < e < f(n) and gcd(f(n),e) = 1, *e.g.*, e = 5
e) Calculate d = e^{-1} mod f(n), *e.g.*, d = 77
f) Public key KU = {e,n} = {5,119}
g) Private key KR = {d,n} = {77,119}
h) Plaintext M = 19
i) Ciphertext C = M^e mod n = 19^5 mod 119 = 66
j) Plaintext M = C^d mod n = 66^{77} mod 119 = 19

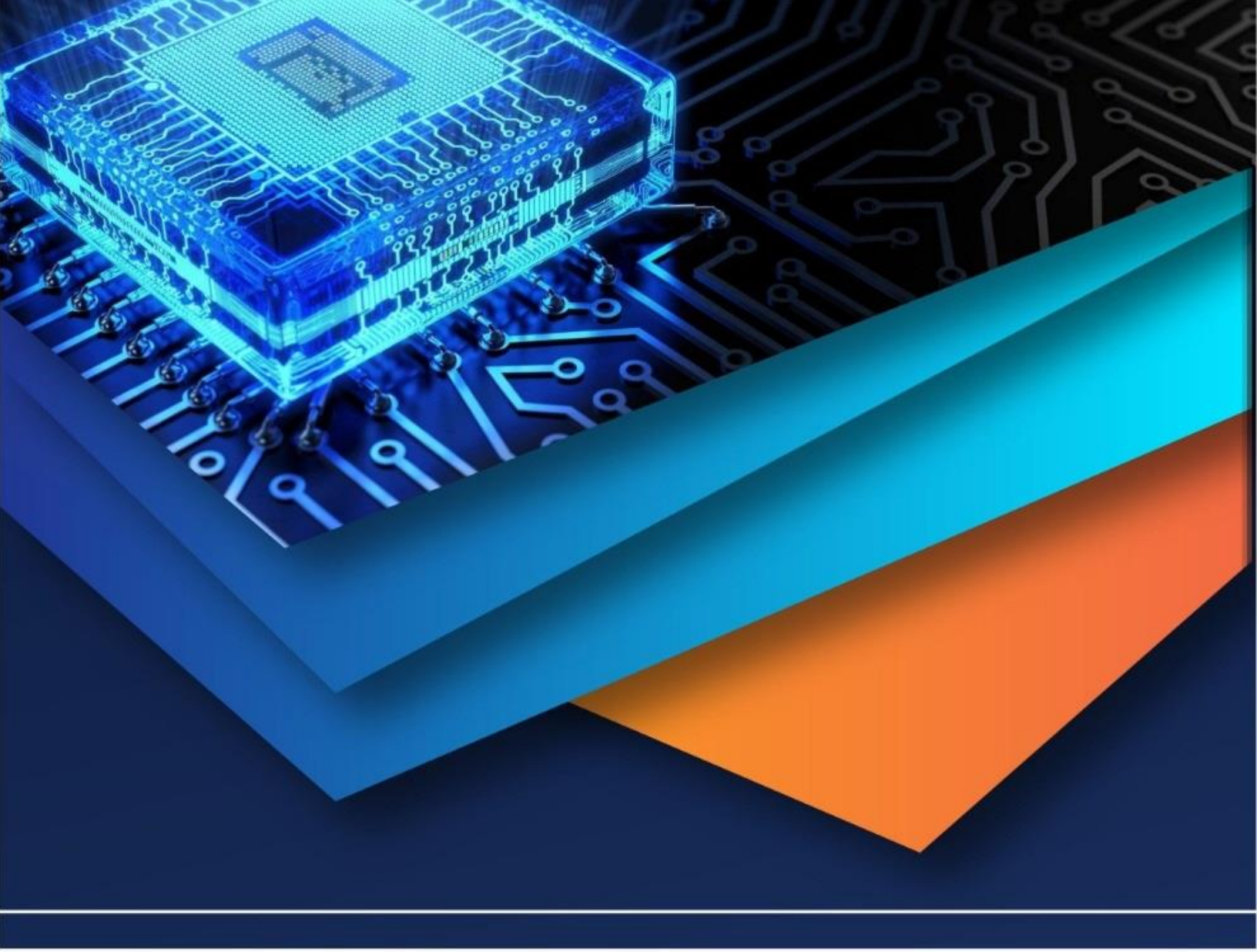
IX. CONCLUSION

Quantum computers are devices that can carry out computations using quantum mechanical properties such as superposition and entanglement. Qubits, quantum bits, are used to described states similar to the bit in transistor-based computing. Transmitting information with access restricted to the intended recipient even if the message is intercepted by other cryptography. Quantum Key Distribution (QKD) is secure, this makes impossible to intercept message without being detected. It is needed for potential applications like faster combinatorial search and simulating quantum systems and prevent decoherence or unwanted interaction with environment.

REFERENCES

[1] IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 44, NO. 6, OCTOBER 1998
[2] IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 47, NO. 1, JANUARY 2001
[3] ION OPTICAL CLOCKS AND QUANTUM INFORMATION PROCESSING
[4] D. J. Wineland, J. C. Bergquist, T. Rosenband, P. O. Schmidt,
[5] IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 47, NO. 1, JANUARY 2001.
[6] IEEE Transactions on Information Theory, Vol. 44, No. 6, p. 2724
[7] The topsy turvey world of quantum computing " By Justin Mullins
[8] http://www.qubit.org
[9] http://www.wired.com/news/technology/0,69033-0.html
[10] http://physicsweb.org/articles/news/9/11/13/1
[11] http://blog.wired.com/gadgets/index.blog?entry_id=1295520
[12] http://www.umich.edu/news/index.html?Releases/2005/Dec05/r121205b
[13] http://news.zdnet.com/2100-1009_22-6026098.html

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)