VOL 3 (2019) NO 1

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Quantum Computing Concepts with Deutsch Jozsa Algorithm

Poornima Aradyamath[#], Naghabhushana N M[#], Rohitha Ujjinimatad[*]

[#] *Department of Physics, RYM Engineering College, Ballari, 583104, India*
[*] *Department of Electronics, Proudhadevarya Institute of Technology, Hosapet, 583225, India*
E-mail: ampoornima@gmail.com, naghabhushananm@gmail.com, rohita_ujjini@rediffmail.com

Abstract— **In this paper, we briefly review the basic concepts of quantum computation, entanglement, quantum cryptography and quantum fourier transform. Quantum algorithms like Deutsch Jozsa, Shor's factorization and Grover's data search are developed using fourier transform and quantum computation concepts to build quantum computers. Researchers are finding a way to build quantum computer that works more efficiently than classical computer. Among the standard well known algorithms in the field of quantum computation and communication we describe mathematically Deutsch Jozsa algorithm in detail for 2 and 3 qubits. Calculation of balanced and unbalanced states is shown in the mathematical description of the algorithm.**

Keywords— **Quantum Computer, Quantum Algorithms, Qubit, Quantum Cryptography**

I. INTRODUCTION

The rapid growth of computer technology is based on standard principles of quantum theory. Today both theoretical and practical machines works based on classical physics. However physics tells us that the quantum computation arena pretty differently. An important goal of quantum algorithms is work more efficiently than classical algorithms to solve the same problem. Fourier transformation techniques are used to achieve the exponential speed-up. Quantum computational speed-up has prompted an awful lot research to build quantum computer systems, to locate new algorithms, to quantify the rate-up, and to separate classical from quantum computation. One important intention is to recognize the purpose for quantum computational speed-up, to understand what assets are needed to do quantum computation [1]. Small quantum-mechanical systems are simulated on quantum computers, however simulation of classical Turing machines of this type can't be predicted to be efficient. A quantum computers makes direct use of Qubits to encode information and perform operation on data according to the laws of quantum mechanics [2]. The performance of the algorithms which run on quantum computer is much better than any classical algorithm.

Quantum systems have the strength to revolutionize information technology by employing quantum computers and quantum cryptography [3, 4]. In general quantum networks [5, 6] have various application ranging from distributed quantum computing [7, 8] and securing data from multiple function evaluation [9, 10]. Over a period of 20 years, the theory quantum algorithms has been an interesting research area for researchers. Although huge quantities of quantum computers are not yet implemented to replace conventional computers. The race for quantum computational supremacy, Google's approach and IBM challenge are examined. The time line of quantum technologies from 2015 to 2045 is shown [11].

II. BACKGROUND IN THEORETICAL AND EXPERIMENTAL DEVELOPMENT OF QUANTUM COMPUTER

In the early 1930's the proposed quantum mechanical computers were power full and produced surprising results than classical computers. First mathematical computation proven in the papers of Chruch and Turning in 1936 underlies the subsequent development of theoretical computer science became the distinction between computable and non computable functions. First mathematical computation, which underlies the subsequent development of much theoretical computer science, was the distinction between computable and non computable functions shown in papers of Chruch [1936] and Turning [1936]. The result of these papers is Chrch's thesis. It concludes that a turning machine can simulate all quantum computing devices. Conjugate coding is first time introduced by Stephen Winser in the year 1960's. However the long term security offered by many encryption systems. It was further developed as public key cryptography by Rabin and Even. Also in 1973 Alexnde Holevo shows that n qubits cannot carry more than n classical bits of information which is referred as Halevo's bound. In 1975 R P Poplavskii showed the computational infeasibility of simulating quantum systems on classical computers due to

superposition principle [12]. Further in 1980's Paul Benioff describes Hamiltonian Models of quantum mechanical computers. Yurimanin proposed further implementation work on quantum computing [13, 14]. Further in 1982 Feynman suggested that quantum computer might be useful for simulating other systems of quantum computing [15, 16]. In 1984 Charles H. Bennett has further played a major role in reversible computing [17]. Next it introduced the Toffli gate which provides a universal set of classical computation with the NOT and XOR gates [18]. Several years later a quantum Turing machine was described by Deutsch and confirmed that quantum computers can be constructed. In 1985 Deutsch developed a notation of quantum mechanical turning machine. Bernstein, Vazirani and Yao showed that quantum computers can do anything a classical can do with at most a small (logarithmic) slow down [19]. Deutsch and Josza generalized this hassle to one that can be solved exactly on a quantum computers in polynomial time, however for which an precise solution on a classical computers calls for exponential time [20, 21, 22].

The early 1990's, first truly quantum algorithms explained, these algorithms with no classical analog that were probably better than any possible classical algorithms. The first of these was Deutsch's algorithms, later generalized to the Deutsch-Jozsa algorithms [21]. These initial quantum algorithms were able to solve problems effetely with certainty that classical techniques can solve effectively with high probability. The same problem can be solved using classical algorithm with high probability in polynomial time. The example for polynomial separation between quantum and classical computation was Bernstein and Vazirani [23].

Daniel R Simon's polynomial time algorithm for a quantum computer distinguishes computable random function from one class and random number of other function where as same task founds to be difficult in the classical turning machine and would take exponential time [24]. The runtime of Simon's first quantum algorithm is found to be optimal and exponentially faster than any equivalent classical algorithm [25]. Despite the fact that his problem seems to be very abstract, it corresponds to large number of problems in the field of computer science, which includes calculating discrete logarithms and factorization of integers into primes [26]. Quantum computers can solve non-oracular problems with exponential speedup over the well known classical algorithms. Finding discrete logarithms and factoring integers are the two problems which are hard to run on classical computers and they have been used frequently in the proposed cryptosystems. Efficient algorithms were given by peter Shor in 1997 to solve these problems on quantum computer [27]. To solve both oracular and non-oracular problems with exponential speedup many generalizations and variations of these algorithms have been discovered by many researchers [28, 29, 30, 31, 32, 33, 34, 35, 36]. Quantum Fourier transform (QFT) is base for these algorithms. Mathematical computation such as factoring of a large integer could be done on a quantum computer. The performance of these tasks is outstanding compare to their performance on classical computer. A novel methods were proposed for implementing public-key cryptosystems but its security is depends on factorization of large integer. Here secure communication can be established with digital signatures instead of carrying the keys [37]. The invention of the Shor algorithm provides exponential speed-up for number of algorithms in public-key cryptosystems because no classical algorithm is faster than Shor's factoring algorithm i.e factorization of integer into prime numbers.

Lov K. Grover presented a quantum mechanical algorithm to search a particular item in large data base. For example to find someone's phone number in telephone directory containing N names with the probability of 0.5 classical algorithm will need to see minimum of N/2 names, where as Grover's quantum search algorithm will complete the same task in $O\sqrt{N}$ steps [38, 39]. These two algorithms created lot of interest in building quantum computer. After this, research in developing quantum algorithms was in steady status for first few years. Further in the year 1998, using Deutsch's algorithms first experimental 2-bit qubit NMR quantum computers are demonstrated by Jonatha A. Jones and Michle Mosca. For instance, in 2001 researchers at NMR Computers reported the successful implementation of Shor's algorithm in a 7-qbit quantum computers [40]. Todd D. Pittman and Jeremy L. O'Brien demonstrate quantum controlled-not gates using only linear optical elements in the year 2003 [41]. From the last decade, entire work carried out in practical implementation of quantum computers compare to theoretical work. First quantum bytes (qubyte) and pure state NMR quantum computers were built in the year 2004. In the same year Jian Wei group constructed five photon entanglement, minimal number of qubits required for universal quantum error correction [42]. Next further in the year 2006 Theoretical physicist and experimentalists have presented 12 qubits quantum information processing extending from 7 qubits to 12 qubits, despite of that, it also explains decoherence.

III. Basic Concepts In Quantum Computation

Quantum bits or Qubits are used to encode the information in the form of ones and zeros in quantum computing. They are in the superposition state with the measurable value of 1 or 0. The mathematical representation of superposition state of the qubit with the base vectors $|0\rangle$ and $|1\rangle$ is given by

$$|\psi\rangle = b_0|0\rangle + b_1|1\rangle$$

Where b_0 is the complex scalar amplitude of measuring $|0\rangle$ and b_1 is the amplitude of measuring the value $|1\rangle$. The normalizing condition for complex coefficients is $b_0^2 + b_1^2 = 1$. $|\psi\rangle$ is the unit vector. Its means that $\||\psi\rangle\| = \langle\psi|\psi\rangle = 1$ i.e. $|b_0|^2 + |b_1|^2 = 1$.

The most computational basis is used in the quantum computing.

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

The base vectors can be represented as

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

A Qubit can be expressed as

$$|\psi\rangle = b_0|0\rangle + b_1|1\rangle$$

$$= b_0\frac{|+\rangle + |-\rangle}{\sqrt{2}} + b_1\frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

$$= \frac{b_0 + b_1}{\sqrt{2}} |+\rangle + \frac{b_0 + b_1}{\sqrt{2}} |-\rangle$$

It's tough to do any exciting computation with only a single qubit. Multiple qubits are used to form quantum registers. The length of quantum registers determines the amount of information they can carry. Since every qubit in quantum register is in the superposition state, the n qubits register is in the superposition of all possible 2^n states. It is represented as

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} b_i |i\rangle$$

Using above expression the states of the qubit register for $n = 3$ is as follows:

$$|\psi_3\rangle = \sum_{i=0}^{2^3-1} b_i |i\rangle$$

$$= \sum_{i=0}^{7} b_i |i\rangle = \sum_{i=0}^{7} b_0|0\rangle + b_0|1\rangle + b_0|2\rangle + b_0|3\rangle + b_0|4\rangle + b_0|5\rangle + b_0|6\rangle + b_0|7\rangle$$

The representation of integer in the string form is

$$|0\rangle = |000\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$$

$$|1\rangle = |001\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = [0\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T$$

$$|2\rangle = |010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = [0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]^T$$

$$|3\rangle = |011\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = [0\ 0\ 0\ 1\ 0\ 0\ 0\ 0]^T$$

$$|4\rangle = |100\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$$

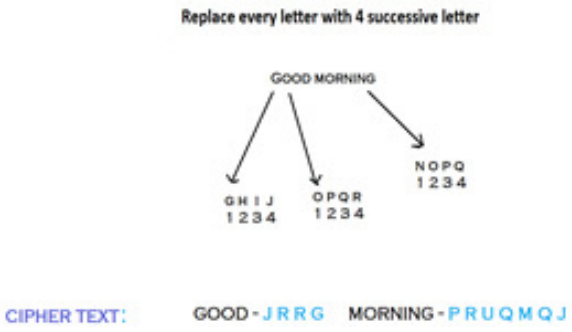
$$|5\rangle = |101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = [0\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T$$

$$|6\rangle = |110\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = [0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$$

$$|7\rangle = |111\rangle = |1\rangle \otimes |1\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T$$

IV. QUANTUM CRYPTOGRAPHY

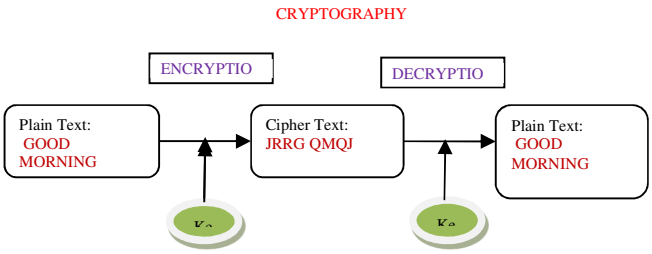
Cryptography is art of writing mathematical logics to encrypt and decrypt the data. It enables us to transmit or store sensitive information is insecure like internet. So that it cannot be reached by anyone except the intended recipient. Let us understand with an example, suppose we need to send information " Good Morning ". This information every letters are replaced with 4th successive letter in the alphabet. The encrypted message will be " JRRG PRUQMQJ ". To decrypt our message we have to go back 4 letters in the alphabets using the letter that we want to decrypt. The transformed image is done in this way,



This process of converting information in garbage non readable format is called encryption. The process opposite to this is known as decryption. Decryption is achieved only with the help of key which is only known by the legitimate recipients. The key is used to decrypt the hidden message. This makes transmission of information more secure because even if the hacker mange to get the information it will not sense to them information stored in the form of CIPHER TEXT.

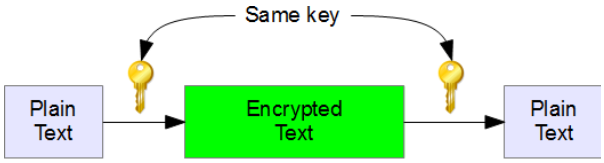
Cryptography is highly intensified field in securing the data. Breaking cipher text is a just primary pencil and paper puzzle in school level. There is an abundant applications in the field of quantum cryptography. It is a popular emerging field in technological age, which includes broadcast, internet, e-mails, network communication cell phones, business finances and private confidential information.

A quantum computer threatens the basic idea of cryptographic security, because it can perform certain kinds of computations that cannot be done by conventional computers. Cryptographic keys can be broken quickly by quantum computers and allow an eavesdropper to hack the secured information. Recently two cryptographic cipher are defined, asymmetric cipher [43]. Symmetric cryptosystem is one in which decryption and encryption is done on the same key where as in asymmetric cryptosystem decryption and encryption processes performed on the mechanism of two different keys [44].



Techinque involved in cryptography

- **Symmetrical (secret-key) cryptosystems**



In symmetric cryptography both receiver and sender perform the task with the same single key. For example Alice sends a message to Bob. Alice encrypted plaintext message has to be decrypt by Bob using the same key, which is used by Alice while encrypting. The key need to be kept secret, it means only Alice and Bob should know it. It is very difficult task to exchanging secrete keys over a public networks. Therefore asymmetric cryptography was introduced to solve this single key distribution problem.

- **Asymmetrical (public-key) cryptosystems**

In this method, each individual has a private key and public key. Two distinct keys are used for encryption and decryption. For instance, if Bob wants to encrypt the message Alice must send her public key to Bob and Bob can would decrypt the message with his private key. In this type of cryptography each has a private key and a public key. Public key is shared with all those whom we need to share the information, but private key is not revealed with everyone it kept secret.

V. Quantum Fourier Transform

Before discussing the quantum Fourier transform, we will talk a bit about the discrete Fourier transform (DFT) as well as the Fast Fourier Transform (FFT) algorithm. The QFT will be constructed to be essentially the equivalent of the FFT with a quantum circuit.

The DFT of a N Point sequence $x(n) = \{x(0), x(1), x(2), \ldots . x(N-1)\}$ is

$$X(K) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\, e^{-j\frac{2\pi kn}{N}}$$

The time domain sequence $x(n)$ can be computed from $X(k)$ using the Inverse Discrete Fourier Transform (IDFT):

$$x(n) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} X(K)\, e^{j\frac{2\pi kn}{N}}$$

Let $W_N = e^{-j\frac{2\pi}{N}}$

$$X(K) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\, W^{kn}$$

The matrix form representation of the DFT equations is

$$X = W_N \; x$$

$$\begin{bmatrix} X(0) \\ X(1) \\ \vdots \\ X(N-1) \end{bmatrix} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W_N^{1} & W_N^{2} & \cdots & W_N^{N-1} \\ 1 & W_N^{2} & W_N^{4} & \cdots & W_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & W_N^{N-1} & W_N^{2(N-1)} & \cdots & W_N^{(N-1)(N-1)} \end{bmatrix}$$

The direct computation of DFT requires N^2 complex multiplications and $N(N-1)$ complex additions. FFT is an algorithm that efficiently computes the DFT. Any FFT algorithm compute DFT with $log_2 N$ complex additions and $\frac{N}{2} log_2 N$ complex additions. FFT algorithms are based on the symmetry properties of twiddle factor W_N. The following are the properties.

$W_N^{K+\frac{N}{2}} = -W_N^{K}$ and $W_N^{K+N} = W_N^{K}$

Quantum Fourier Transform (QFT) is a quantum implementation of the discreet Fourier transform. quantum algorithms which are computing DFT are exponentially faster than FFT of classical computers.

The QFT for N=8 of the function

$$|f\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)$$

$$= \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$QFT_N\ (|f\rangle)\ = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & W_8^{\,1} & W_8^{\,2} & W_8^{\,3} & W_8^{\,4} & W_8^{\,5} & W_8^{\,6} & W_8^{\,7} \\ 1 & W_8^{\,2} & W_8^{\,4} & W_8^{\,6} & W_8^{\,8} & W_8^{\,10} & W_8^{\,12} & W_8^{\,14} \\ 1 & W_8^{\,3} & W_8^{\,6} & W_8^{\,9} & W_8^{\,12} & W_8^{\,15} & W_8^{\,18} & W_8^{\,21} \\ 1 & W_8^{\,4} & W_8^{\,8} & W_8^{\,12} & W_8^{\,16} & W_8^{\,20} & W_8^{\,24} & W_8^{\,28} \\ 1 & W_8^{\,5} & W_8^{\,10} & W_8^{\,15} & W_8^{\,20} & W_8^{\,25} & W_8^{\,30} & W_8^{\,35} \\ 1 & W_8^{\,6} & W_8^{\,12} & W_8^{\,18} & W_8^{\,24} & W_8^{\,30} & W_8^{\,36} & W_8^{\,42} \\ 1 & W_8^{\,7} & W_8^{\,14} & W_8^{\,21} & W_8^{\,28} & W_8^{\,35} & W_8^{\,42} & W_8^{\,49} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$QFT_N\{\,|f\rangle\} = \frac{1}{\sqrt{2^3}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} & -j & -\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} & -1 & -\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & j & \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} \\ 1 & -j & -1 & j & 1 & -j & -1 & j \\ 1 & -\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} & j & \frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} & -1 & \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & -j & -\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & -j & \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & -1 & \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & j & -\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} \\ 1 & j & -1 & -j & 1 & j & -1 & -j \\ 1 & \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & j & -\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}} & -1 & -\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} & -j & \frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

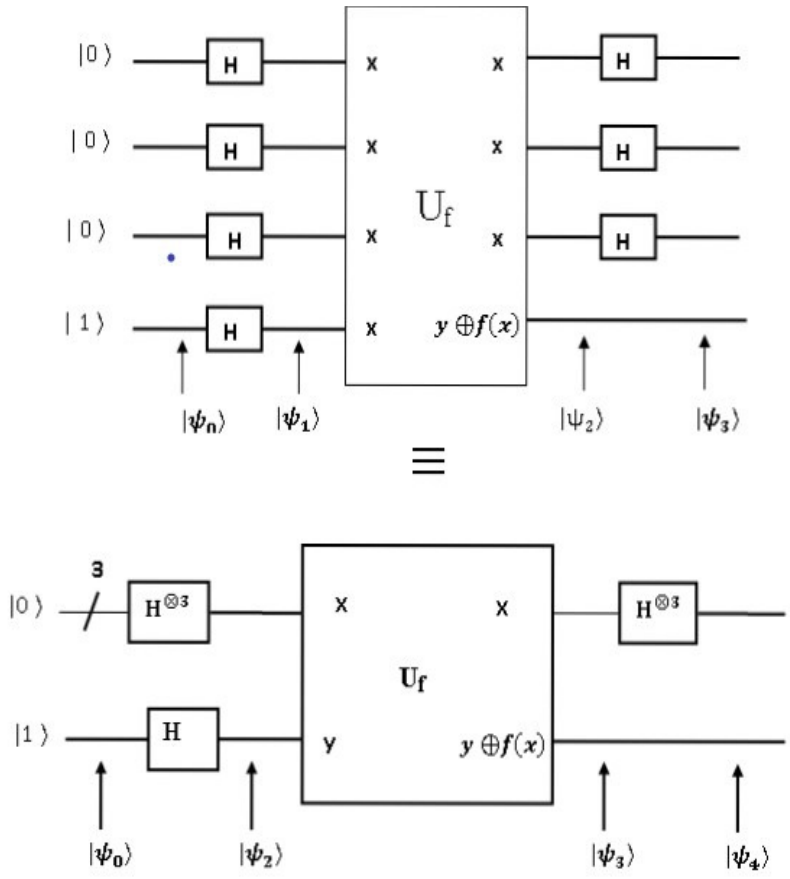


Fig 1: Circuit for implementing Deutsch Jozsa Algorithm

VI. QUANTUM ALGORITHMS

The quantum computation of few quantum algorithms shows that computational speed is much faster than any classical algorithm. Hence research on finding new quantum algorithms has been the spread all across the quantum computation field.

The discovery of the following types of quantum algorithms shows better performance and their advantages over known classical algorithms:

- QFT based algorithms. e.g. Integer factorization and discrete logarithm of Shor and Deutsch Josza Quantum algorithm
- Grover's data search quantum algorithm and its extentions.
- Algorithms to simulate quantum systems.

Deutsch–Jozsa problem and its quantum algorithm

Deutsch-Jozsa Problem: A Boolean function $f:\{0,1\}^n \to \{0,1\}$ is said to be constant if the output $f(x)$ equals to 0 or 1 for all values of input x. It is said to be balanced if $f(x)$ equals 0 for exactly half of the entire possible x, and 1 for the other half. Our problem is to distinguish between these two cases. The four possible functions of $f(x)$ are

$$\underbrace{f(x)=0 \quad f(x)=1}_{constant\ functions} \qquad \underbrace{f(x)=x \quad f(x)=\bar{x}}_{balanced\ functions}$$

This algorithm distinguishes constant from balanced functions in one evaluation of f, versus $2^{n-1}+1$ evaluations for classical deterministic algorithms. Balanced functions have many interesting and some useful properties.

The Deutsch-Jozsa Problem is specifically designed to be easy for quantum algorithm and hard for any deterministic classical algorithm. The motivation is to show a black box problem that can be solved efficiently by a quantum computer with no error, where as a deterministic classical computer would need exponentially many queries to the black box to solve the problem. Although of little practical use, it is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm. The generalization of Deutsch algorithm is known as Deutsch Jozsa algorithm.

The solution for Deustch-Jozsa algorithm is based on the expression given in the equation (1) which solves with probability 1 using only one call to the quantum black box computing $f(x)$. A traditional classical algorithm would require two calls to a classical black box in order to determine if $f(x)$ is constant or balanced.

$$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle \tag{1}$$

The algorithm flow is shown in the figure 1. This circuit uses an n-qubit query-register prepared in the state $|0\rangle$ and answer-register prepared in $|1\rangle$. The Hadamard transformation is applied to each qubit. The function f is embedded in an oracle U_f and this is followed by another Hadamard transformation on each query-register qubit. The measurement at the end will test positive for $|0\rangle$ if f was constant, and negative if f was balanced.
The states through the circuit are as follows:

The input state $|\psi_0\rangle$ is

$$|\psi_0\rangle = |0\rangle\ |0\rangle\ |0\rangle\ |1\rangle = |0\rangle^{\oplus 3}|1\rangle \tag{2}$$

The state $|\psi_1\rangle$ is the output of the Hardmard gate for the input state $|\psi_0\rangle$ which is given as

$$|\psi_1\rangle = H^{\oplus 4}|0\rangle^{\oplus 3}|1\rangle = H|0\rangle\ H|0\rangle H|0\rangle H|1\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.\begin{bmatrix}1\\0\end{bmatrix}.\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.\begin{bmatrix}1\\0\end{bmatrix}.\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.\begin{bmatrix}1\\0\end{bmatrix}.\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.\begin{bmatrix}0\\1\end{bmatrix}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}.\frac{1}{\sqrt{2}}.\begin{bmatrix}1\\1\end{bmatrix}.\frac{1}{\sqrt{2}}.\begin{bmatrix}1\\1\end{bmatrix}.\frac{1}{\sqrt{2}}.\begin{bmatrix}1\\-1\end{bmatrix}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle).\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle).\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

Where $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^3}}(|0\rangle+|1\rangle).(|0\rangle+|1\rangle).(|0\rangle+|1\rangle).|-\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^3}}\{|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle + |101\rangle+|110\rangle+|111\rangle\}.|-\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^3}}\sum_{x\in\{0,1\}^3}|x\rangle\left[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right]$$

The transformation U_f is applied on the state $|\psi_1\rangle$

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

$$|\psi_2\rangle = U_f\frac{1}{\sqrt{2^3}}\{|000\rangle+|001\rangle+|010\rangle+|011\rangle + |100\rangle+|101\rangle+|110\rangle + |111\rangle\}\left[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}}\{|000\rangle[|f(000)\oplus|0\rangle - |f(000)\oplus|1\rangle] + |001\rangle[|f(001)\oplus|0\rangle - |f(001)\oplus|1\rangle] + |010\rangle[|f(010)\oplus|0\rangle - |f(010)\oplus|1\rangle] + |011\rangle[|f(011)\oplus|0\rangle - |f(011)\oplus|1\rangle] + |100\rangle[|f(100)\oplus|0\rangle - |f(100)\oplus|1\rangle] + |101\rangle[|f(101)\oplus|0\rangle - |f(101)\oplus|1\rangle] + |110\rangle[|f(110)\oplus|0\rangle - |f(110)\oplus|1\rangle] + |111\rangle[|f(111)\oplus|0\rangle - |f(111)\oplus|1\rangle]\}$$

There are three cases

1. $f(000) = f(001) = f(010) = f(011) = f(100) = f(101) = f(110) = f(111) = 0$
2. $f(000) = f(001) = f(010) = f(011) = f(100) = f(101) = f(110) = f(111) = 1$
3. Half of $f(000), f(001), f(010), f(011), f(100), f(101), f(110), f(111)$ equal to 0 and another half equal to 1.

N=2, m=2^2=4

Applying case (1)

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}}\{|000\rangle[|0\rangle - |0\oplus|1\rangle] + |001\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |010\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |011\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |100\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |101\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |110\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |111\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle]\}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}}\{|000\rangle[|0\rangle - |1\rangle] + |001\rangle[|0\rangle - |1\rangle] + |010\rangle[|0\rangle - |1\rangle] + |011\rangle[|0\rangle - |1\rangle] + |100\rangle[|0\rangle - |1\rangle] + |101\rangle[|0\rangle - |1\rangle] + |110\rangle[|0\rangle - |1\rangle] + |111\rangle[|0\rangle - |1\rangle]\}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^3}}\{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\}\left[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right]$$

Applying case (2), all functions are 1 then $|\psi_2\rangle$ state becomes

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}}\{|000\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |001\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |010\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |011\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |100\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |101\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |110\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |111\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle]\}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}}\{|000\rangle[|1\rangle - |0\rangle] + |001\rangle[|1\rangle - |0\rangle] + |010\rangle[|1\rangle - |0\rangle] + |011\rangle[|1\rangle - |0\rangle] + |100\rangle[|1\rangle - |0\rangle] + |101\rangle[|1\rangle - |0\rangle] + |110\rangle[|1\rangle - |0\rangle] + |111\rangle[|1\rangle - |0\rangle]\}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^3}}\{-|000\rangle - |001\rangle - |010\rangle - |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle\}\left[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right]$$

For case (3): half of the functions are 0 and another half are 1; let *f(000)= f(001)= f(010)= f(011)= 0* and *f(100)= f(101)= f(110)= f(111)=* 1 so that the $|\psi_2\rangle$ state becomes

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}}\{|000\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |001\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |010\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |011\rangle[|0\oplus|0\rangle - |0\oplus|1\rangle] + |100\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |101\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |110\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle] + |111\rangle[|1\oplus|0\rangle - |1\oplus|1\rangle]\}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^4}} \{|000\rangle[|0\rangle - |1\rangle] + |001\rangle[|0\rangle - |1\rangle] + |010\rangle[|0\rangle - |1\rangle] + |011\rangle[|0\rangle - |1\rangle] + |100\rangle[|1\rangle - |0\rangle] + |101\rangle[|1\rangle - |0\rangle] + |110\rangle\,[|1\rangle - |0\rangle] + |111\rangle[|1\rangle - |0\rangle]\}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^3}} \{|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle\} \left[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right]$$

The results of all three cases can be expressed as

$$|\psi_2\rangle = \frac{1}{\sqrt{2^3}} \sum_{x\in\{0,1\}^3} (-1)^{f(x)}\,|x\rangle \left[\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right]$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^3}} \sum_{x\in\{0,1\}^3} (-1)^{f(x)} \;\; \frac{1}{\sqrt{2^3}} \sum_{y\in\{0,1\}^3} (-1)^{x\,.\,y}\;\; |y\rangle$$

Interchanging the order of summation, we get

$$|\psi_3\rangle = \frac{1}{\sqrt{2^3}} \sum_{y\in\{0,1\}^3} \frac{1}{2^3} \sum_{x\in\{0,1\}^3} (-1)^{x\,.\,y + f(x)}\;\; |y\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2^3}} \sum_{y\in\{0,1\}^3} \left(\frac{1}{2^3} \sum_{x\in\{0,1\}^3} (-1)^{x\,.\,y + f(x)}\right) |y\rangle$$

In the above equation each state has amplitude (A_{amp}) i.e

$$A_{amp} = \frac{1}{2^3} \sum_{x\in\{0,1\}^3} (-1)^{f(x)}$$

$$\left|\frac{1}{2^3} \sum_{x\in\{0,1\}^3} (-1)^{f(x)}\right|^2 = \begin{cases} 1 & If\;\; f\;\; is\;\; constant \\ 0 & If\;\; f\;\; is\;\; balanced \end{cases}$$

TABLE 1
STATUS OF TWO QUBIT SYSTEM FUNCTION

f_{00}	f_{01}	f_{10}	f_{11}	State
0	0	0	0	Constant
0	0	0	1	Unbalanced
0	0	1	0	Unbalanced
0	0	1	1	Balanced
0	1	0	0	Unbalanced
0	1	0	1	Balanced
0	1	1	0	Balanced
0	1	1	1	Unbalanced
1	0	0	0	Unbalanced
1	0	0	1	Balanced
1	0	1	0	Balanced
1	0	1	1	Balanced
1	1	0	0	Balanced
1	1	0	1	Unbalanced
1	1	1	0	Unbalanced
1	1	1	1	Constant

VII. CONCLUSION

This paper briefly represents the history of the quantum computer development, experimental demonstration of quantum computers and basic concepts in quantum computation. Quantum cryptography and quantum fourier transform are described. Among the well know quantum algorithms, Deutsch–Jozsa quantum algorithm is described mathematically in detail for 3 qubits. Here output of each stage is shown to find the whether the system function is balanced or unbalanced. Table represents the status of the system for 2 qubits. Similarly we can show for 3, 4 and 5 qubits systems.

REFERENCES

1. Niklas Johansson, Jan-Åke Larsson *Efficient classical simulation of the Deutsch– Jozsa and Simon's algorithms,* Quantum Inf Process (2017) 16:233, DOI 10.1007/s11128-017-1679-7
2. Nielsen M and Chuang I. *Quantum computation and Quantum information*. Cambridge Univ. press Cambridge, 2000.
3. Thaddeus D. Ladd, Fedor Jelezko, Raymond Laflamme, Yasunobu Nakamura, Christopher Monroe, Jeremy L. O'Brien, Quantum Computers, Nature 464, March 2010, PP 45-53
4. Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, REVIEWS OF MODERN PHYSICS, 2002.
5. L. M. Duan and C. Monroe. "Quantum networks with trapped ions". In: *REVIEWS OF MODERN PHYSICS* 82.2 (Apr. 2010), pp. 1209–1224.
6. H J Kimble. "The quantum internet". In: *Nature 453* (June 2008), pp. 1023–1030. ISSN: 0028-0836.
7. J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Optimal local implementation of nonlocal quantum gates, Physical Review A, vol. 62, no. 5, Nov. 2000.
8. Joseph F. Fitzsimons Naomi H. Nickerson and Simon C. Benjamin. "Freely Scalable Quantum Technologies Using Cells of 5-to-50 Qubits with Very Lossy and Noisy Photonic Links". In: *PHYSICAL REVIEW X* 4.4 (Dec. 2014).
9. Michael Ben-Or, Claude Crepeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith, Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority, 47th IEEE Annual Symposium on Foundations of Computer Science (FOCS 2006), October 2006.
10. MicheleMosca Artur Ekert. "The Hidden Subgroup Problem and Eigenvalue, Estimation on a Quantum Computer". In: *Procceedings of 1st NASA International Conference on Quantum Computing and Quantum Communication,* vol. 1509. Lecture Notes in Computer Science. 1999.

11. Cristian S. Calude and Elena Calude, The Road to Quantum Computational Supremacy, arXiv:1712.01356v1 [quant-ph] 4 Dec 2017
12. R P Poplavskii. “Quantum Computers”. In: 1975. Chap. Thermo dynamical models of information processing, pp. 465–501.
13. Paul Benioff. “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by turning machines”. In: *Journal of stastical physics* (1980).
14. Vychislimoe Manin YU and I nevychislimoe. “Computable and Non computable (in Russian). Sov.Radio.” In: (Archived from the original on May 10,2013. Retrieved 2013-03-04.), pp. 13–15.
15. R P Feyman. “Simulating Physics with Computers”. In: *International Journal of Theoretical Physics* 21.6 (1982), pp. 467–488.
16. J. G. Hey. *Feynman and Computation – Exploring the Limits of Computers*. Perseus Books, 1999.
17. Bennet. C H. “Logical reversibility of computation”. In: *IBM Journal of Research and Development* (1973).
18. T. Toffoli. *Reversible computing in Automata, Languages and Programming, Seventh Colloquium, Lecture Notes in Computer Science*. Ed. By J. W. De Bakker and J. van Leeuwen. Vol. 84. Springer, 1980.
19. Yao. “Quantum circuit complexity”. In: *Proceeding of the 34th IEEE Symposium on Foundations of Computer Science*. 1993, pp. 352–361
20. D. Deutsch. “Quantum theory, the Church-Turing principle, and the universal quantum computer”. In: *Royal Society London* (1985).
21. D. Deutsch and R. Jozsa. “Rapid solution of problems by quantum computation”. In: *Royal Society London* (1992).
22. David Deutsch. “Quantum Theory as a Universal Physical Theory”. In: *International Journal of Theoretical Physics* 24.1 (1985).
23. E. Bernstein and U. Vazirani. “Quantum complexity theory”. In: *Proceedings of 25th ACM Symposium on Theory of Computating*. 1993, pp. 11–20.
24. D. Simon. “On the power of quantum computation”. In: *35th IEEE Symposium on the Foundations of Computer Science*. 1994.
25. Natacha Portier Pascal Koiran Vincent Nesme. “A quantum lower bound for the query complexity of Simon’s problem”. In: Lecture Notes in Computer Science, vol 3580. Springer, Berlin, Heidelberg (Jan. 2005), pp. 1287–1298.
26. Richard Jozsa. “Quantum Factoring, Discrete Logarithms, and the Hidden Subgroup Problem”. In: *Computing in Science and Engineering* 3.2 (Mar. 2001), pp. 34–43.
27. P. W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings of 35th IEEE Symposium on Foundations of Computer Science*. IEEE, Nov. 1994.
28. Wim van Dam and Sean Hallgren. “Efficient Quantum Algorithms for Shifted Quadratic Character Problems”. In: *quant-ph/0011067* (2001).
29. Michele Mosca, Artur Ekert. “The Hidden Subgroup Problem and Eigenvalue Estimation on a Quantum Computer”. In: *Procceedings of 1st NASA International Conference on Quantum Computing and Quantum Communication,* vol. 1509. Lecture Notes in Computer Science. 1999.
30. F. Magniez G. Ivanos and M. Santha. “Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem”. In: *quant-ph/0102014* ().
31. S Hallgren. “Polynomial-time quantum algorithms for Pell’s equation and the principal ideal problem.” In: *In Proceedings of the 34th ACM Symposium on the Theory of Computing (STOC)*. 2002, pp. 653–658.
32. John Watrous J Niel De Beaudrap Richard Cleve. “Sharp quantum versus classical query complexity separations”. In: *Algorithmica* 34.4 (Jan. 2002), pp. 449–461.
33. Yu. Kitaev. “Quantum measurements and the Abelian Stabilizer Problem”. In: *quant-ph/9511026* (2008).
34. Russell S. Hallgren and A. Ta-Shma. “Normal subgroup reconstruction and quantum computation using group representations.” In: *In Proceendings of 32nd ACM Symposium on the Theory of Computing*. 2000, pp. 627–635.
35. J. Watrous. “Quantum algorithms for solvable groups”. In: *In Proceedings of the. 33rd ACM Symposium on the Theory of Computing*. 2001, pp. 60–67.
36. M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani, “Quantum mechanical algorithms for the nonabelian hidden subgroup problem” *In Proceedings of 33rd Annual ACM Symposium on Theory of Computing,* 2001 pp. 68-74
37. L. Adleman R. L. Rivest A. Shamir. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Communications of the ACM* 21.2 (Feb. 1978), pp. 120–126
38. L. K. Grover. “A fast quantum mechanical algorithm for database search”. In: *In Proceedins of the 28th Annual ACM Symposium on the Theory of Computing, ACM, New York,* 1996, pp. 212–219.
39. L. K. Grover. “Quantum mechanics helps in searching for a needle in a haystack”. In: *Physical Review Letters* 79.325 (July 1997).
40. Vandersypen L M, Steffen M, Breyta G, Yannoni CS, Sherwood MH, Chuang I L. “ Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance ” Nature. 2001 Dec 20-27;414 (6866):883-7.
41. Pittman T. B, Fitch M. J., Jacobs B. C. and Franson, J. D. “Experimental controlled-not logic gate for single photons in the coincidence basis” *Physical Reviews A*, volume 68, number 032316, 2003.
42. Zhao, Zhi, Chen, Yu-Ao, Zhang, An-Ning, Yang, Tao, Briegel, Hans J, Pan, Jian-Wei. ” Experimental demonstration of five-photon entanglement and open-destination teleportation ” Nature, volume 430, no. 6995, pp 54-58, July 2004.

43. Rose H, and Hag J, " Using a Cipher Key to Generate Dynamic S-Box in AES Cipher System " International Journal of Computer Science and Security, 6, pp 19-28, 2012.

44. Sekar A., Radhika, S. and Anand, K. " Secure Communication Using 512 Bit Key " European Journal of Scientific Research, 52, pp 61-65, 2012