# Grover's QSA based MC-CDMA Detector

Saif H. Abdulnabi, M.Sc.
Electrical Engineering Department,
College of Engineering, University of Baghdad,
Baghdad, Iraq

Saleem M. R. Taha, Ph.D.
Electrical Engineering Department,
College of Engineering, University of Baghdad,
Baghdad, Iraq

## ABSTRACT

Multi-Carrier Code Division Multiple Access (MC-CDMA) is considered as one of the major techniques used in 4G broadband wireless services. It combines the advantages of the OFDM systems, of robustness to the multi path effects, and the advantages of CDMA systems, which are high privacy and security. However, a problem appears in the detection of transmitted information because of the effect of noise, fading and other multipath effects. In this paper, Grover's quantum search algorithm based MC-CDMA detector is proposed as a solution for this problem. Grover's quantum search algorithm is based on the concepts of quantum computing, such as quantum bit, quantum register and quantum parallelism. The performance of the proposed detector was realized and compared with previous works. The simulation results showed the superiority of the proposed detector in BER performance. The performance of the proposed detector showed that it is very close to the optimum.

## Keywords

MIMO-OFDM, MC-CDMA, GROVER'S QSA

## 1. INTRODUCTION

Since the last years of previous century the search started on communication systems that are capable on accommodate multiple users with high bit rate but the spectrum of frequency is limited. The search grows rapidly when wireless local area networks (WLANs) appear extensively and the internet growth becomes exponential. New methods for obtaining high capacity wireless networks are proposed. One of the major important techniques proposed for this objective is the orthogonal frequency division multiplexing (OFDM). This technique was proved to be optimal in combating the inter-symbol interference (ISI) and inter carrier interference (ICI) by using cyclic prefix [1]. For this proof, it is more robust for multipath effects and more spectral efficient because the bandwidth of the communication system is divided into small overlapping sub-carriers, which save much bandwidth and reduce the effects of the multipath propagation.

Another important technique that appeared using code division multiple access (CDMA) has many benefits such as multi access capability, protection against multipath interference, privacy of transmission, interference and jamming rejection, and low probability interception [2]. Recently, the MC-CDMA system was proposed to combine these benefits with the natural robustness to frequency selective fading offered by OFDM [3]. A problem appears in the detection of transmitted information because of finding the effect of noise, fading and other multipath effects, which necessitates the use of an equalizing technique to equalize the effect of the wireless channel. The solution for this problem is proposed here by introducing the Grover's quantum search algorithm based MC-CDMA detector. The concepts and principles of quantum computing are used to find the solution.

This paper is organized as follows, a theoretical analysis will be given for the MC-CDMA systems in section 2. In section 3, Grover's QSA is introduced. The structure of Grover's QSA based MC-CDMA detector and the procedure of this algorithm to find the solution will be discussed in section 4. The simulation results of the proposed MC-CDMA detector will be given in section 5. Finally, the most important conclusions about the proposed MC-CDMA detector proposed in this paper will be discussed in section 6.

## 2. MC-CDMA SYSTEM

Multi Carrier Code Division Multiple Access is a combination of two main sub systems, which are direct sequence CDMA (DS-CDMA) and orthogonal frequency division multiplexing (OFDM), this system allows supporting multiple users at the same time [4]. The first system is the DS-CDMA system where the information bearing from individual users are spread, summed, and fed to the second system acted by the OFDM system. In OFDM stage the data will be modulated to orthogonal sub-carriers to be broadcasted through the channel. The two stages of the MC-CDMA system are discussed in the coming subsections.

### 2.1 DS-CDMA Stage

Direct Sequence-Code Division Multiple Access is a multi-access technique where the data signal is directly modulated by the code signal. The resulting signal modulates the wideband carrier. It is from direct multiplication that the DS-CDMA gets its name [2]. This is done when multiple users access the shared medium using the same bandwidth at the same time but by different orthogonal codes. These orthogonal codes are high rate streams used to spread the users data over wide spectrum. This operation is occurring by multiplying each user data stream by one of codes in order to perform the spreading function that enable variable data rate transmission [5]. Figure (1) shows the block diagram of CDMA transmission stage.

The spreading process for the data of users has benefits, which are increasing link privacy and reducing the probability of jamming or detection. Therefore, the data cannot be extracted or interfered without knowing the spreading codes. After the spreading operation, the spread data from multiple users are added and fed to the OFDM modulator stage as the next process.

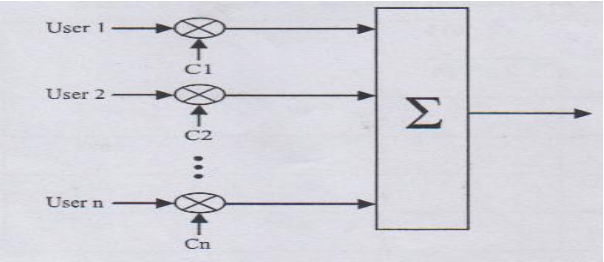

**Fig 1: Block diagram of CDMA transmission stage.**

## 2.2 OFDM Stage

The OFDM stage is started after the CDMA stage, where the output data is encoded , mapped by a certain modulation scheme, and converted from serial form to parallel form via S/P convertor. After conversion to parallel streams, data sub-streams are fed to the IFFT block; therefore, the parallel stream will modulate the overlapping orthogonal sub-carriers. This modulation has the benefit of reducing the multipath effect, since sub-carriers bandwidth is narrow that it will approximately experience a flat fading which leads to a small amplification in the detection process at the receiver. Moreover, to the robustness to the multipath effects, the modulation of data on orthogonal sub-carriers saves much bandwidth because the sub-carriers are allowed to overlap, that increased the spectral efficiency of the system. After process of the IFFT is finished, the modulated streams are converted to serial form via P/S convertor. Cyclic prefix is added to the packet to eliminate any possible ISI or ICI, then the resulted signal is transmitted throuh the channel. Figure (2) shows the structure of OFDM transmitter.

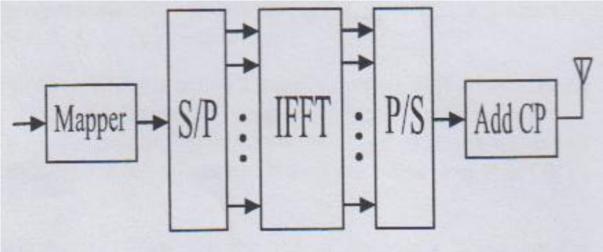

**Fig 2: OFDM transmitter stage.**

# 3. GROVER'S QUANTUM SEARCH ALGORITHM

## 3.1 Foundation of Quantum Computation

The smallest unit of information stored in a two-state quantum computer is called a quantum bit or qubit [6]. A qubit is a unit vector in the two-dimensional Hilbert complex vector space for which a particular basis, denoted by {|0>, |1>}, has been fixed. The orthonormal basis {|0>, |1>} can be expressed as $\{(1, 0)^T, (0, 1)^T\}$. For the purposes of quantum computation, the basis states |0> and |1> are taken to represent the classical bit values 0 and 1 respectively. Unlike the classical bit however, a qubit can be in a linear superposition of |0> and |1> such as [7]:

$$|\varphi> = a|0> + \; b|1> = (a\;, b)^T \qquad \cdots(1)$$

where $a$ and $b$ are complex numbers and called probability amplitudes. If we measure this superposition with respect to the basis {|0› , |1›}, the probability of getting the measured value |0› is $|a|^2$, and the probability that the measured value |1› is $|b|^2$ [8]. Since these are only two possibilities, a and b are required to satisfy $|a|^2 + |b|^2 = 1$.

Combining $< \varphi \mid$ and $|\psi>$ as in $< \varphi \; |\psi>$, denotes the inner product of the two vectors, it is a scalar. For instance, <0|0> = <1|1> =1, <0|1> = <1|0> = 0. The notation $| \; \varphi \; ><\psi|$ is the outer product of $|\varphi>$ and $|\psi>$, it is an operator [6].

A system of $n$ qubits is called an $n$-bit "quantum register" (Qregister). An $n$-bit Qregister | ψ > is set up from qubits spanned by |i>, i = 0… ($N$-1), $|i>$ is computational basis, where $N=2^n$ states can be stored in the Qregister at the same time [9], [10], described as:

$$|\psi_n\rangle = \sum_{i=0}^{2^n-1} a_i \, |i\rangle \qquad \cdots(2)$$

For instance, a three-qubit system (three-bit Qregister), | i > would range from |000> to |111>. By consequence, the three-bit Qregister of (5) contains the information of eight states [6].

An $n$-qubit Qregister | ψ > has a state space of $2^n$ dimensions. It is this exponential growth of the state space with the number of particles that suggests a possible exponential speed-up of computation on quantum computers over classical computers [6].

It is worth mentioning that any linear hermitian operator **U** operating on a qregister is executed parallel on all $2^n$ stored states, which is called quantum parallelism. **U** must be unitary [6].

## 3.2 How Grover's QSA works

There are large problems can be specified as search problems of the form "find some x in a set of possible solutions such that statement f(x) is true". Conventionally the only way to do a search is to systematically examine all the possibilities until you find the solution. Clearly if the search space has N entries, then the time taken to complete a search is $O$ (N). No classical algorithm can do better than this. Only Quantum search algorithms alone can do better than $O$ (N). Grover's QSA is one of these quantum algorithms that works in time $O$ ($\sqrt{N}$). For large N, this could yield very large performance increases [11].

Grover's QSA starts with a quantum register of n qubits, where n is the number of qubits necessary to act the search space of size $2^n$ = N, all initialized to |0›:

$$|0\,\rangle^{\otimes n} = |0\rangle \qquad \cdots(3)$$

The first step is to put the system into an equal superposition of states, this is achieved by applying the Hadamard transform $H^{\otimes n}$, applying n applications of the elementary Hadamard gate:

$$|\psi\rangle = \; H^{\otimes n} \, |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \qquad \cdots(4)$$

The coming series of transformations is often referred to as the Grover iteration, and performs the amplitude amplification. The Grover iteration will be repeated ( $\frac{\pi}{4}\sqrt{2^n}$) times. The first step in the Grover iteration is a call to a quantum oracle, O, which will modify the system depending on whether it is in the configuration we are searching for. An oracle is basically a black-box function, and this quantum oracle is a quantum black-box, meaning it can observe and modify the system without collapsing it to a classical state, that will recognize if the system is in the correct state or not. The oracle's task in Grover's QSA is that of finding and marking the specific correct state. The oracle may be described algebraically by an (N x N) element matrix with all the non-zero elements lying on its diagonal. The diagonal elements of oracle matrix may assume the values of +1 or -1 as shown [12]:

$$O = \begin{bmatrix} \pm1 & 0 & \cdots & 0 \\ 0 & \pm1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \pm1 \end{bmatrix} \qquad (5)$$

If the system is in fact in the correct state, then the oracle will rotate the phase by $\pi$ radians, otherwise it will do nothing, effectively marking the correct state for further modification by subsequent operations. We must remember that such a phase shift leaves the probability of the system being correct state the same, although the amplitude is negated. The oracle function is expressed as shown:

$$|x\rangle \overset{O}{\rightarrow} (-1)^{f(x)}\ |x\rangle \qquad \cdots (6)$$

Where f(x) = 1 if x is the correct state, and f(x) = 0 otherwise.

The second step of Grover iteration is call diffusion transform, which performs inversion about the average (amplitude amplification), transforming the amplitude of each state so that it is as far above the average as it was below the average prior to the transformation, and vice versa. This diffusion transform consists of three parts that are: firstly, another application of the Hadamard transform $H^{\otimes n}$, secondly followed by a conditional phase shift that shifts every state except $|0\rangle$ by -1, thirdly followed by yet another Hadamard transform.

We can act the diffusion transform as shown in equation (10):

$2\,|0\rangle\langle 0| - I$: (represent the conditional phase shift) ⋯(7)

$[2\,|0\rangle\langle 0| - I]\,|0\rangle = 2\,|0\rangle\langle 0|0\rangle - I = |0\rangle$ ⋯(8)

$[2\,|0\rangle\langle 0| - I]\,|x\rangle = 2\,|0\rangle\langle 0|x\rangle - I = -\,|x\rangle$ ⋯ (9)

The equation of entire diffusion transform, using the notation $|\psi\rangle$ from equation (4) is:

$$H^{\otimes n}\,[2\,|0\rangle\langle 0| - I]\,H^{\otimes n} = 2\,H^{\otimes n}\,|0\rangle\langle 0|\,H^{\otimes n} - I = 2\,|\psi\rangle\langle\psi| - I \quad (10)$$

In addition, the entire equation of Grover iteration is:

$$[2\,|\psi\rangle\langle\psi| - I]O^{R} \qquad \cdots\ (11)$$

When the Grover iteration is completed a classical measurement is performed to determine the result, which will be correct with probability very close to (1) and completing the execution of the algorithm. The overall runtime of entire Grover's QSA is $(\frac{\pi}{4}\sqrt{N})$.The circuit diagram for Grover's QSA is shown below.

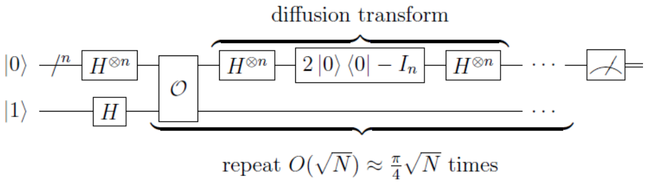

**Fig 3: Circuit diagram for Grover's QSA. [11]**

Moreover, a high-level circuit depiction of Grover’s QSA is shown figure (4):

We can summarized Grover's QSA nicely as follows:

Inputs:

1- A quantum oracle O which performs the operation O $|x\rangle = (-1)^{f(x)}\ |x\rangle$, where

f(x) = 0 for all $0 \le x < 2^{n}$ except $x_o$, for which $f(x_o) = 1$.

2- n qubits initialized to the state $|0\rangle$.

Output: $x_o$
Run time: $\frac{\pi}{4}\sqrt{2^{n}}$ operations, with probability of access very close to (1).

Moreover, the procedure of Grover's QSA can be written as follows:

1- $|0\rangle^{\otimes n}$ ≡ Initial state.

2- $H^{\otimes n}\ |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^{n}}}\sum_{x=0}^{2^{n}-1}|x\rangle = |\psi\rangle \equiv$ apply the Hadamard transform to all qubits.

3- $[(2\,|\psi\rangle\langle\psi| - I)\,]O^{R}\,|\psi\rangle \approx |x_o\rangle$ ≡ apply the Grover iteration R $\approx \frac{\pi}{4}\sqrt{2^{n}}$ times.

4- $x_o$ ≡ measure the register.

## 4. GROVER'S QSA BASED MC-CDMA DETECTOR

When the transmitted data reach to the receiver, the data will be distorted by the effect of noise, fading, and multipath propagation, which is essential to use equalizing techniques to repeat the original data streams. The first process in the MC-CDMA receiver is removing the cyclic prefix from the received packets. Because of applying this operation, any possible of ISI or ICI will be eliminated. Then the received data stream is converted to parallel form via S/P converter and fed to the FFT block, because the FFT process is done to the parallel streams. After that the data is fed to the Grover's QSA processor as equalization process , this process retrieves the original streams. the Grover's QSA follows a certain procedure in order to find the solution and equalize the received streams. This procedure can be summarized by the following steps:

**Step 1. Initialize the quantum register.** Initialize the factors $(a\,,b)$ of each quantum bit in the quantum register; this is done by assigning a value of $\frac{1}{\sqrt{2}}$ to be represented as linear superposition of all possible states.

**Step 2. Superposition of state.** Obtain the probability matrices by squaring the values of quantum register because p(0) = $a^{2}$, p(1) = $b^{2}$. This operation is done by making all register as an equal superposition of states achieved by applying Hadamard transform $H^{\otimes n}$ which requires n applications of the elementary Hadamard gates.

**Step 3. Assigning process.** Start the bit assigning process by using the uniform distribution based random number generation code (randi). The upper limit of (randi) is 100 that will be multiplied by the probability of zero in order to perform bit assigning. As an example, if the probability of zero for certain quantum bit is 0.12 then if the random number generated by the (randi) command is equal to or less than 12 then assign that bit to the value 0, else assign it to 1.

**Step 4. Fitness function.** Evaluate the set of solutions based on maximum likelihood condition that is regarded as the fitness function, where the lowest error among the groups of registers, which are 16 groups, will be the target group for the model ends. The description of this condition is the square of the Euclidean distance between the received stream and the desired value of original stream must be as minimum as possible. The fitness function condition is expressed in equation (12).

$$E = \arg\min \|y - h.x\|^{2} \qquad \cdots(12)$$

Where (*y*) is the received stream, (*h*) is the channel response matrix, and *(x)* is the set of possible solutions provided by Grover's QSA processor.

**Step 5. Quantum rotation gate.** Update the groups of quantum registers using quantum rotation gate that its value equals 0.005 $\pi$ . In order to direct the quantum bits toward the target group, ensure steady convergence to the solution, and avoid the false convergence, which leads to errors. In other words the rotation quantum gate makes registers converge to the optimum solution.

**Step 6. Grover iteration.** Apply Grover iteration, which is equal to $[\frac{\pi}{4}\sqrt{2^n}]$. In our model, n = 4 which refers to number of bits in each case of register. In order to obtain the optimal solution the number of Grover iterations are equal to three, because ( $\frac{\pi}{4}\sqrt{2^4} = \pi = 3.14 \cong 3$).

**Step 6.1. Selective Inversion.** Apply quantum oracle that is stated by equation (6).

**Step 6.2. Inversion about Average.** Apply diffusion transform that is stated by equation (10).

**Step 7. Measurement.** Measure the quantum register state. The measurement result will be the desired state that is the optimal solution, which will appear with highest amplitude and probability is very close to one.

After finding the solution by Grover's QSA processor, the equalized stream is converted from parallel form to serial form using a parallel to serial convertor. After that, the received stream is de-mapped by one of de-mapping techniques. When the de-mapping is complete, the first stage of reception of data is complete.

Figure (5) shows the first stage of the MC-CDMA receiver.

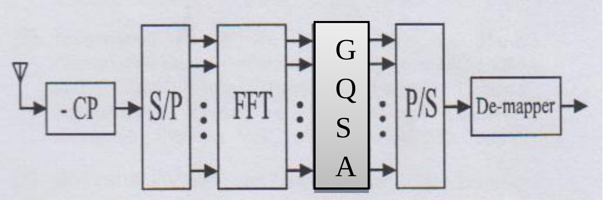

**Fig 5: First stage of MC-CDMA receiver.**

After repeating the desired data stream, the main data stream is fed to the CDMA demodulator. Each user will take his data stream through multiplying the main by the same code used to spread his data stream at the transmission. After that, the resulted samples is summed and fed to a limited detector in order to restructure the data stream for each user. Figure (6) shows the second stage of MC-CDMA receiver.

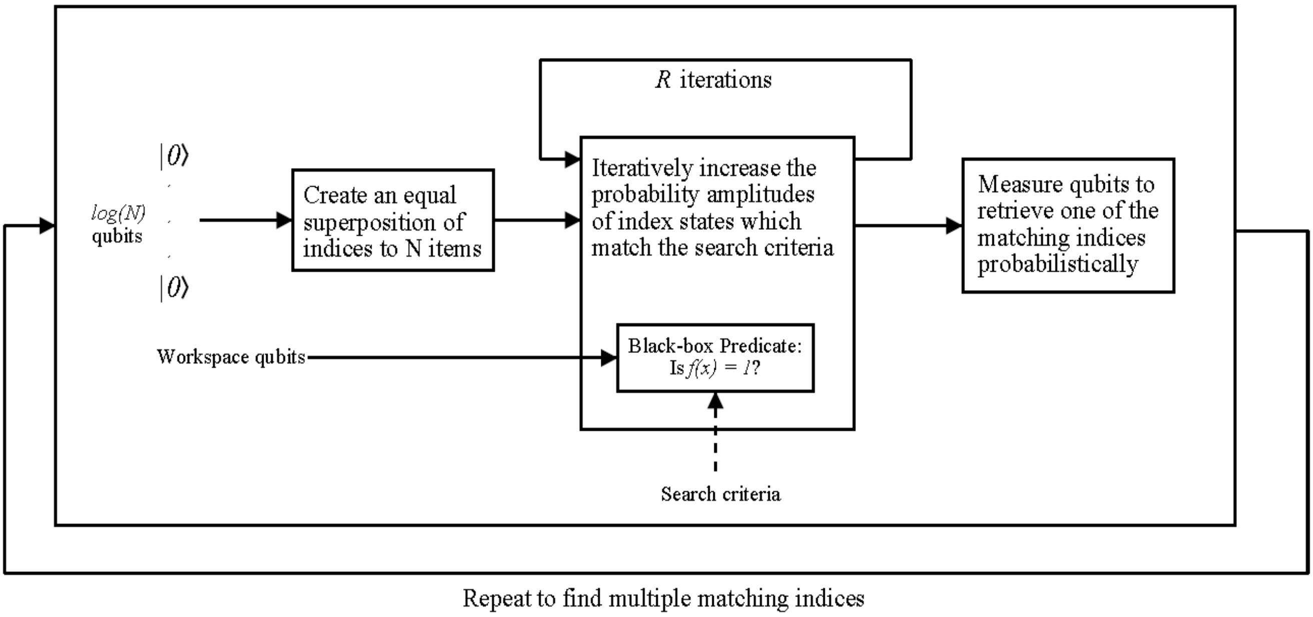
R iterations
|0⟩
log(N) qubits
|0⟩
Create an equal superposition of indices to N items
Iteratively increase the probability amplitudes of index states which match the search criteria
Measure qubits to retrieve one of the matching indices probabilistically
Workspace qubits
Black-box Predicate: Is f(x) = 1?
Search criteria
Repeat to find multiple matching indices

**Fig 4: A high-level circuit depiction of Grover's QSA. [13]**

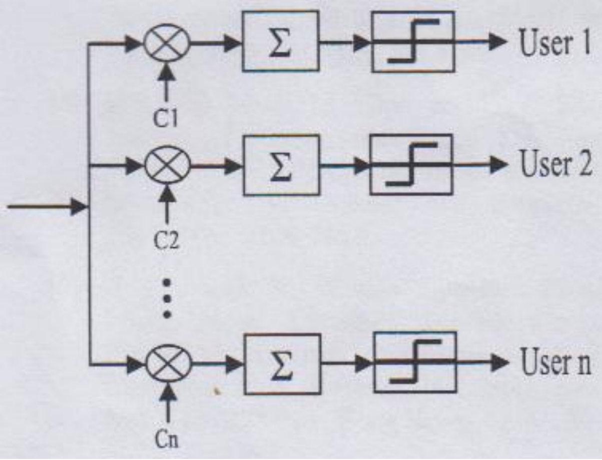

**Fig 6: Second stage of MC-CDMA receiver.**

The proposed system was done with computer simulations through programming MATLAB 2014a.The number of users that was used in proposed system is 4. The spreading code set was Walsh codes set. BPSK and QPSK were used respectively as mapping schemes. Cyclic prefix of 25% was used to eliminate any possible ISI, ICI, and multipath effects. The bandwidth was divided to 16 sub-carriers using 16 IFFT code. The channel characteristics was assumed to be unknown and a channel estimation process was performed through the use of pilot carriers.

In order to explain the improvement in BER performance that obtained by the using Grover's QSA based MC-CDMA detector, a comparison was made with GD based 4x4 MIMO-OFDM system proposed in [6] for both BPSK and QPSK mapping schemes. Figure (7) shows the performance results of the proposed Grover's QSA based MC-CDMA detector beside with the GD based 4x4 MIMO-OFDM detector proposed in [6] for both BPSK and QPSK mapping schemes.

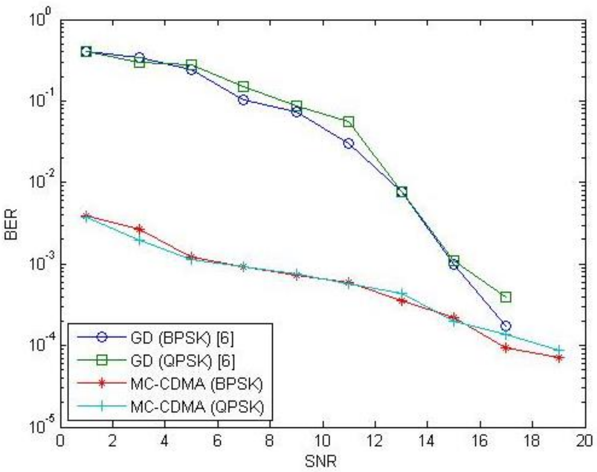

**Fig 7: BER performance for various Grover's QSA based detector.**

## 5. CONCLUSION

In this paper, the whole explanation on the MC-CDMA structure was given. The benefits of the MC-CDMA system over the classical OFDM system was stated.

The Grover's quantum search algorithm (Grover's QSA) was also showed in detail and giving its procedure to find the optimum solution by taking $O(\sqrt{N})$ steps to search the solution of $N$ items, that no classical algorithm can do better than $O(N)$.

The design of the Grover's QSA based MC-CDMA detector was introduced, the most important parameters for the proposed detector were given and comparison was held between the Grover's QSA based MC-CDMA detector and GD based 4x4 MIMO-OFDM detector. The results show that the Grover's QSA based MC-CDMA detector has outperformed the GD based 4x4 MIMO-OFDM detector proposed in [6] by 9 dB for BPSK and 7 dB for QPSK, which proves that the proposed detector is better in BER performance than the QGA based MC-CDMA detector proposed in [6].

## 6. REFERENCES

[1] V. J. Naveen, K. M. Krishna, and K. R. Rajeswari, “Performance analysis of equalization techniques for MIMO systems in wireless communication”, International Journal of Smart Home, Vol.4, No.4, pp. 47-63, October 2010.

[2] R. V. Nee, and R. Prasad, “OFDM for Wireless Multimedia Communications”, Artech House Inc., Norwood, MA, USA, 2000.

[3] M. Faisal, J. Uddin, and I. H. Haider. “Simulation Based Performance Analysis of MC-CDMA and CDMA over Rayleigh Fading Channel”, International Journal on Internet and Distributed Computing System, Vol.2, No.1, pp. 120-122, 2012.

[4] B. Kulhare, and P. Sihna. “Simulation and Analysis of CDMA system under AWGN and Rayleigh Fading Channel”, International Journal of Computers and Technology, Vol.6, No.2, pp. 336-342, 2013.

[5] M. A. Abu-Rgheff, “Introduction to CDMA Wireless Communications”, Elsevier Ltd., 2007.

[6] F. Lei, L. Zhou, L. Liu, and H. Li. “Quantum Search Based Signal Detection for MIMO-OFDM Systems”, 18th International Conference on Telecommunications, pp. 276-281, 2011.

[7] M. A. Nielsen and I. L. Chuang. “Quantum Computation and Quantum Information”, 10th edition, the United Kingdom: Cambridge University press, 2010.

[8] E. Gazioglu. “Grover Algorithm”, M.Sc. Thesis in Applied Mathematics and Computer Science, Eastern Mediterranean University, Gazimagusa, North Cyprus, February 2011.

[9] S. Imre and F. Balázs, “Quantum multi-user detection”, Proc. 1st. Workshop on Wireless Services & Applications, pp.147–154, 2001.

[10] S. Imre and F. Balázs, “Non-coherent Multi-user Detection based on Quantum Search”, Proc. of IEEE Int. Conf. on Communication (ICC) pp.283-287, 28 April – 2 May 2002, New York, USA.

[11] E. Strubell, “An Introduction to Quantum Algorithms”, COS498-Chawathe, Springer, 2011.

[12] P. Botsinis, S. X. NG, and L. Hanzo. “Quantum Search Algorithms, Quantum Wireless, and a Low-Complexity Maximum Likelihood Iterative Quantum Multi-User Detector Design”, IEEE access, vol. 1, pp. 94-122, 2013.

[13] G. F. Viamontes, Igor L. Markov, and John P. Hayes, “Is Quantum Search Practical?”, 5th proceedings of the IEEE CS and the AIP, pp. 22-30, Michigan, USA, 2005.