Evolution of Quantum Computing Based on Grover's Search Algorithm

Prakhar Shrivastava, Kapil Kumar Soni and Akhtar Rasool
Computer Science Engineering
Maulana Azad National Institute of Technology
Bhopal, India

Abstract— **Quantum computing introduces an efficient way for unfolding complex problems on computing systems. It uses concept of superposition and entanglement, & hence supports intrinsic parallelism for obtaining the speedup in context of time over classical computing. Quantum algorithms can be efficiently implemented over quantum computing system. Most popular quantum algorithms like Grover's and Shor's provide a great foundation to specifically design the algorithms. These algorithms work on improving the lower runtime bounds of classical algorithms. Grover's algorithm exhibits a quadratic polynomial speedup while searching an element among 'N' elements unstructured database. The algorithmic strategy can be applied over various computer science related applications and some important are being considered in this article i.e. pattern matching, data mining and machine learning. This article explores quantum fundamentals; history based evolution followed by Grover's search algorithm in detail with cascading advantages, limitations & applications and also finally concludes with the significance of quantum computing & quantum algorithmic domains.**

*Keywords— **Quantum Computing; Grover's Algorithm; Pattern Matching; Qubit; Superposition; Data Mining; Machine Learning;***

I. INTRODUCTION

Technology advancements in areas like science, defense, biomedical require fast computations which cannot be provided by classical computers. There are various complex problems that can be solved by using high-performance computers. One of the kinds is based on the usage of quantum effects on computers. Quantum computing uses quantum mechanics and considered as an elemental part of physics. One of the main problems with classical computers is to deal with the parallelism. There are different concepts which are introduced to cope up with stall in computing like multithreading, multi cores and so on. At large level, parallelism is attained using distributed environment, clustering, grid computing, etc. In other words, Parallelism is forced by providing various external logics which slows the computation. But in quantum computing parallelism is intrinsic feature provided by its architecture [1, 12].

Most popular quantum algorithms like Shor's and Grover's provided a great background to give something to quantum computers to process. These algorithms use phenomena of quantum mechanics like superposition and entanglement to provide a computational speedup. Shor's quantum algorithm runs on a factorization problem and provides output substantially faster than generic algorithm, in time O((log N)^3). RSA public-key cryptosystem depends on stiffness of integer factorization. Shor's algorithm implies that this cryptosystem is vulnerable to attack by quantum computer. Grover's algorithm provides optimization to one of the basic problem in computer science i.e. unstructured search. Any classical algorithm will take O(N) time for this task while Grover's quantum algorithm will generates the result in $O(\sqrt{N})$. It provides polynomial time speed up over generic search algorithms [1, 16].

II. QUANTUM FUNDAMENTALS

A. *Quantum Bits*

In classical computers, digital signal represents 0 and 1 states as one bit information. Two bit represents four states 00, 01, 10, 11 and n bit represents 2^n states. In quantum computers, a quantum bit is used called 'Qubit'. It is a two state system which represents one bit information. For example, an electron is used as a Qubit. A spin-down and spin-up of electron can represent 1 and 0 state respectively. Quantum computers perform various arithmetic and logical operations as classical algorithms using Qubits. The main difference is Qubit can represent the superposition of 0 and 1 states. The intrinsic parallelism arises in quantum computing because each Qubit constitute two states at a time, three Qubits can represent eight states simultaneously and becomes capable of performing exponential computations in just single step [5, 12, 17].

B. *Quantum Superposition*

Qubit exhibits a quantum mechanics feature known as superposition. Qubit can represent superposition of 0 and 1. Qubits can be in both the states (i.e. 0 and 1) simultaneously but, in a classical computer there is only a state as 0 or 1. Qubit can be mathematically represented as-

$$\text{X or Y}=|0\rangle \text{ or } |1\rangle$$

The above representation shows that Qubit X is 0 and Qubit Y is 1. The $|0\rangle$ and $|1\rangle$ are the column vectors and can be visualized as-

$$|0\rangle = \binom{0}{1} \text{ and } |1\rangle = \binom{1}{0}$$

When we represent 0 and 1 as the column vectors $|0\rangle$ and $|1\rangle$ respectively, such a superposition is viewed as a linear combination of $|0\rangle$ and $|1\rangle$ as-

$$X=a|0\rangle + b|0\rangle \tag{1}$$

"$|\ \rangle$" is vocalizing as "Ket Vector" and coefficients 'a' and 'b' are called probability amplitude. $|a|^2$ and $|b|^2$ indicates the probability of the Qubits. And hence –

$$|a|^2 + |b|^2 = 1 \quad (2)$$

This means Qubit X is measured in ket 0 with probability $|a|^2$ and also it is measured in ket 1 with probability $|b|^2$ [5, 9].

Generally, we process the input of a superposition state representing four states in one step to get the superposition of four outcomes. When we calculate the output Qubits, the quantum mechanical superposition is destroyed and each Qubit is observed either as 0 or 1. As a result we only get one of the four possible outcomes: 00, 01, 10, and 11(For n = 2) with the same probability. Accordingly, the superposition of Qubits is decided by probability, and the calculation is necessary to determine which one of the possible states is represented [5, 10].

C. Quantum Entanglement

Entanglement phenomena exhibit by Qubits, if electrons are referenced as a Qubit then the distance between electrons i.e. either near or far will give some intuitions i.e. by calculating the first Qubit it will tell something about second Qubit. This implies that entangled bits cannot be expressed as independent of each other.

This property can be used to generate numerous amount of computing power. For instance, classical computers stores one of the 2^n possible outcomes at a time when an n-bit register is used but quantum computers can store all possibilities at a time. Ex -

$$X=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) \quad (3)$$

In the above equation we can infer that second Qubit will have equal probability to exist in either 0 or 1 state if the first Qubit is not measured. But if it has been measured then the second Qubit will have the probability of 0 or 100% [1].

D. Quantum Gates

In quantum computers, Information is processed with the help of logic gates. Quantum gates are the fundamental building block of every operation, different gates are available and each gate is having a specific purpose. These gates are used to transit a Qubit value from one state to another depending on the characteristics of the quantum gate used. Quantum gates are mathematically represented as transposition matrices, or linear operators and all such operators are unitary. The quantum gates are reversible in nature. This nature provides the energy efficiency and it maintains the quantum property that is, entanglement. Few important universal quantum gates used in quantum computing are shown below [1].

a. The Hadamard Gate

One of the most important gates is single-Qubit Hadamard gate often referred to as a "fair coin flip".

$$\boxed{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{|0\rangle\ +\ |1\rangle}{\sqrt{2}}|0\rangle + \frac{|0\rangle\ -\ |1\rangle}{\sqrt{2}}|1\rangle \quad (4)$$

Fig.1 Hadamard Operator

The Hadamard operator applied to a given Qubit with value $|0\rangle$ or $|1\rangle$ will induce an equal superposition of $|0\rangle$ and $|1\rangle$ states. Hadamard operator conducts a rotation of $\pi / 2$ about y-axis followed by rotation of π Radians about x- axis on the block sphere model [1].

b. The Walsh-Hadamard gate

This gate is basically a multi-Qubit Hadamard gate which is used to apply on a multiple Qubits to induce an equal superposition of $|0\rangle$ and $|1\rangle$ states. This operator is used when there is a requirement of working in multiple Qubits environment [7].

c. The controlled-NOT gate

The CNOT gate is a 2 bit reversible gate which works similar as a classical NOT gate with a slight difference which is the use of controlled bit. The control bit must be 1 in order to perform a NOT operation. The diagram depicts that it is having two inputs (c, t) and two outputs (c`, t`). The example of such gate is –

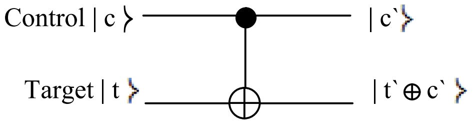

Fig.2 CNOT Gate

d. The controlled-controlled-NOT gate

This reversible gate is a 2 bit gate which uses two control bits and it will perform the operation on target bit 't' if and only if both of the control bits are enabled (i.e. set to 1). This gate is given by 'Tommaso Toffoli' hence also known as 'Toffoli' gate. It is having 3 inputs (c_1, c_2, t) and three outputs ($c`_1$, $c`_2$, t`). [1, 11]

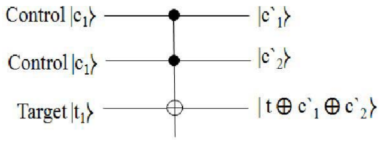

Fig.3 CCNOT Gate

III. Evolution of Quantum Computing

The fundamentals of the quantum world were laid down by the introduction of black body radiations in the early 19th century. But the first milestone was achieved in 1935 by the introduction of the phenomena called quantum entanglement. 1970's were the time when 'Quantum Information Theory' term was coined. In 1980, Richard Feynman stated that a whole new line of computers are required which will work on the phenomena of quantum mechanics and also he had given a basis and fundamental mode of quantum computers. But building quantum computers, computational machines which uses quantum effects was tricky and very huge task to accomplish as no one was sure how to use quantum mechanics to achieve computational speedup. The development went on slowly and 1990's was the huge leap in this area as in 1994 Peter Shor gives a break and introduced an algorithm which will unravel the discrete logarithms and factoring integers on quantum computers. Later on, in 1997 Grover's also had given an interesting break through by introducing an algorithm which deals with searching in unstructured database. In 2001, implementation over quantum computing has begun and IBM and Stanford University first witnessed the carrying out of Shor's algorithm which factorized 15 number using Qubits in nuclear spin. In 2010, first commercial quantum computer was made by D-Wave. It was having 128-Qubit processor but there was no significant increase in the computational speed as compared to classical computers. In 2015, D-Wave introduced a 1000+ Qubits quantum computer which is D-Wave 2x. It is based on 2048 Qubits but half of them not enabled which are enabled later on. Recently IBM launches an IBM cloud which hosts quantum computing environment with the help of quantum circuits [2, 3].

A. Grover"s Algorithm

The problem taken by Grover to apply his algorithms is – There is an unstructured database consists of N records out of which one record will come out to satisfy the desired condition and we have to extract out that record. It is possible to infer that record satisfies the condition or not only after that record is examined. The classical algorithm will visit each record in the database and figures out whether it satisfies given condition or not. If it does stop; if it does not, keep track of that record in case it would not be visited again [6, 11].

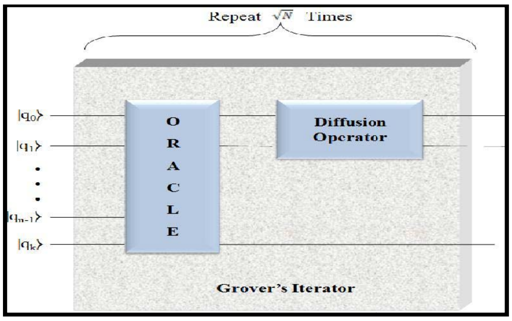

Fig.4 Grover's Iterate Operator

Grover's Algorithm:

```
Step1:  Initialization of Qubit Register
        $|q_0\, q_1\, q_2 \bullet \;\; \bullet \;\; \bullet\, q_{n-1}\rangle \;\longleftarrow\; |0\,0\,0 \bullet \;\; \bullet \;\; \bullet\, 0\rangle$
Step 2: Put system into an equal superposition of states
        $|q_0\, q_1\, q_2 \bullet \;\; \bullet \;\; \bullet\, q_{n-1}\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}}\, b_0|0\rangle + b_1|1\rangle + \bullet \;\; \bullet \;\; \bullet + b_{n-1}|n-1\rangle$
                        // Where $b_0, b_1 \ldots b_{n-1}$ are the probability amplitudes
Step 3: For (i = 1 to $\frac{\pi}{4}\sqrt{\frac{N}{p}}$ by +1)
        {                                       // p = # of elements
            3.1 Amplitude marking using Oracle Operator
                $|b_k\rangle \rightarrow (-1)^{f(b_k)}|b_k\rangle$
                    // Such that $|b_k\rangle \varepsilon \langle q_0\, q_1\, q_2 \bullet \;\; \bullet \;\; \bullet\, q_{n-1}\rangle$
            3.2 Amplification using Diffusion Operator
                $|\mu\rangle \leftarrow \sum_{i=0}^{n-1} b_k$
                        // Computing Amplitude Mean
                $|b_k\rangle \leftarrow (2\mu - |b_k\rangle)$
                    // Re-calculating the probability amplitudes
        }
Step 4: Measure the Output Register
```

The above steps show that how this algorithm will find the desired element. This algorithm can be better understood by designing the architecture of the algorithm. Below is the basic circuit of the Grover's search algorithm.

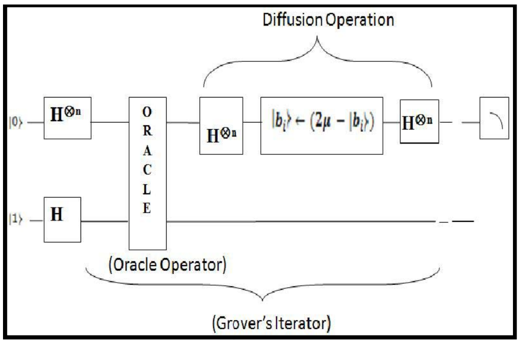

Fig.5 Working of Diffusion Transform

B. Analysis og Grover"s search

Grover's algorithm starts with a quantum registers of 'n' Qubits where n is the number of Qubits represents search space of size N = 2^n, all initialized to |0⟩.

$$\underbrace{|0\rangle \quad |0\rangle \quad \bullet \quad \bullet \quad \bullet \quad |0\rangle}_{\text{(Up to 'n' times)}} \qquad (1)$$

Now, we have to put the system into an equal superposition of states which can be done by Hadamard gate $H^{\otimes n}$. The next block of transformation is referred as 'Grover's iteration' and the task of this transformation is amplitude amplification. According to Grover, in order to achieve the best probability that the desired state is the correct one, we need to rotate the phase by $\left(\frac{\pi}{4}\right)$ radians which can only be possible after $\left(\frac{\pi}{4}\sqrt{2^n}\right)$ iterations and hence Grover's iteration is repeated $\left(\frac{\pi}{4}\sqrt{2^n}\right)$ times. Initially the oracle call is required to configure the searching criteria, and it can observe, modify and recognize whether the system is in correct state or not, if the condition satisfies then it rotates the phase by π radians, otherwise it will do nothing. This phase shift negates amplitude not changing the probability [1, 4].

Average of amplitudes

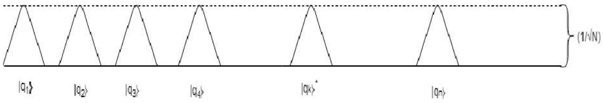

Fig.6 Equal Superposition of all states

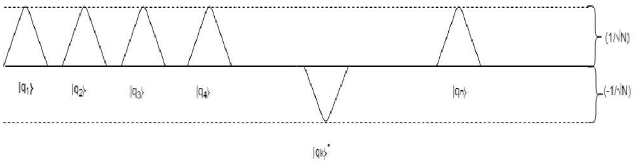

Fig.7 Oracle Negates Marked State Amplitude

The subsequent part of the Grover's algorithm is diffusion operation, which performs inversion about mean, transforming the amplitude of each state so that it will flip upside down and vice versa. This diffusion operation uses a Hadamard gate $\mathrm{H}^{\otimes n}$, followed by a phase shift yet another Hadamard gate. Considering the running time complexity of the algorithm, the exact runtime taken by oracle function varies according to the problem and implementation. So an oracle function $\mathcal{F}_O$ can be considered as a constant time operation. So the total runtime of a single Grover's iteration is$\mathrm{O}(2n)$, from two Hadamard gates, plus cost of conditional phase shift that is $\mathrm{O}(n)$. It can be seen that the total runtime complexity of Grover's algorithm, performing $\mathrm{O}(\sqrt{N}) = \mathrm{O}(\sqrt{2^n}) = \mathrm{O}\left(2^{\frac{n}{2}}\right)$ iterations each with a runtime of $\mathrm{O}(n)$ is $\mathrm{O}\left(2^{\frac{n}{2}}\right)$ [5, 14].

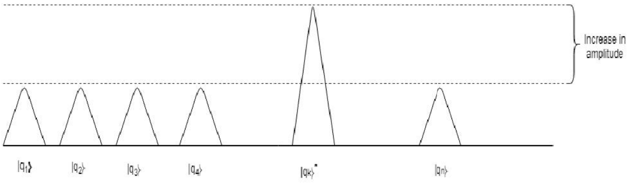

Fig.8 Amplitude Amplification over Desired State

IV. Related Works

A. Related Applications

These Quantum algorithms can be used in various computer science related applications. These algorithms, when utilizes efficiently on the desired architecture, can provide a significant change in dealing with the problems. Grover's search algorithm can be used in various applications like Triangle finding, Boolean Satisfiability, Graph coloring, TSP (Travelling Salesman Problem), Pattern matching problem. Fundamental application of the Grover's search is unsorted database search which is used by various search engines to extract a webpage. Grover's search provides the faster search as compared to the algorithms we are having right now [8].

B. Pattern Matching

This specific application is taken under consideration to fetch some more knowledge of working Grover's search algorithm. This problem states that – Given a text 't' of length 'n' and a pattern 'p' of length 'm' where m $\leq$ n, we need to find out whether the pattern 'p' is in the text 't' or not. Now if we take classical approach, there are various algorithms exist like KMP (Knuth-Morris-Pratt), Boyer-Moore which provide the various solutions. The KMP algorithm provided the solution which will give the output in $\mathrm{O(m\ +\ n)}$ in the worst case. Clearly, this is the optimal solution in the case of classical computing as it will check every character of the text and pattern, to see whether the pattern is present in the given text or not. Finding a pattern in text is analogous to searching an element in unsorted database but the only problem is checking that the text position, for an occurrence of the pattern takes O(n) time. This can be speeded up by taking whether particular pattern matches with the particular text position similar to finding a match in a database. This can be performed in $O(\sqrt{n})$ time with constant failure probablity. So, the overall time complexity is $O(\sqrt{nm})$. Thus, if the pattern occurs in a text then it can be returned with the improved time complexity. We will consider a basic oracle which will compare the text and pattern in constant time. Our goal is to generate oracles with the help this oracle which will solve the string matching problem in $O(\sqrt{m} \ + \ \sqrt{n})$. These oracles are probabilistic which means they will give the correct answer with the constant probability [8].

C. Data Mining

Data preprocessing is the first step of data mining in which data is transformed into a format which is very effective and easy to process. Data preprocessing techniques are mainly used to obtain high quality mining results. Data can be obtained from various sources and most of the data is not of use when the data is gathered for a knowledge gain. So, It must be cleaned and normalize before applying data mining techniques. Different features in a given dataset may have different ranges. So we need to transform the data so that its processing is simple and efficient. To serve this purpose data normalization is performed. Data normalization is a technique used to convert the data into the given small specified range. Clearly, if we are having a dataset of 'N' elements then the classical Min-Max normalization will take O (N) time as it has to access each element and change it to the given specified range. But a significant speedup may be achieved when the same algorithm is implemented in quantum environment.

D. Machine Learning

Machine learning is a streamlined application of artificial intelligence which provides machine the ability to learn itself without being explicitly programmed. There are certain fundamental operations which are generally used in machine learning algorithms which are fast fourier transform, matrix inversion, and eigen decomposition. Quantum variant also goes through the same operations but the difference in computation comes when these series of operations are computed in a fast manner as compared with classical approach. Grover's search plays a very important role in some of the clustering algorithms to search the cluster in very efficient time and help it gaining an exponential speedup. K-Means clustering algorithm needs to search the cluster in order to assign the elements to the cluster. When these clusters are searched with the help of grover's search it will provide the quadratic speedup and help gaining the overall exponential speedup [13, 15].

E. Motivation

The most important thing to save today is time and as we talk about computers and algorithms we define the most efficient algorithm to be the one who takes minimum amount time to solve a particular problem. If we talk about the grover's search algorithm it will provide the solution of most of the real time problems and in addition, it provides quadratic speeup. After learning about Grover's algorithm it has been found out that this algorithm can be used in various applications and also, works efficiently better when compared to existing classical algorithms. The motivation behind structuring this paper is to figure out and show about the vast usage of Grover's search algorithm in computer science domain. And, also we have provided an insight about the recent popular fields in which it can be used and also witness the carrying out the certain elementary operations faster than their classical variants.

V. CONCLUSION

The parallel computational processing can efficiently solve the existing problems, but to achieve such parallelism additional supporting machine architectures are required in classical computers, whereas the quantum computers utilizes super-computational capabilities provided by quantum mechanical superposition property, thus the system can allow exponential operations to be done in parallel and hence we can obtain computational speed-ups through available quantum specific machine architecture. This article contributes the quantum specific fundamentals description and evolved around the historical background of quantum computation and assures that the technological advancement of quantum computers will definitely revolutionize the future computational paradigm, but we cannot expect such highly capable machines as the replacements of classical computers as they are based on probabilistic computations.

The illustration of quantum circuits prove that they all are universal logic gates which are reversible and unitary both. One of the efficient utilization of such circuits was used by Grover's search algorithm and could obtain quadratic polynomial search time speedup. The algorithm along with the circuit description and complexity analysis are discussed in the article, and finally concludes with the various relevant application domains like pattern matching and data mining that can achieve computational speedups using Grover's algorithm.

As far as the limitation of Grover's search algorithm is concerned, it is limited only for unstructured databases, if the databases are structured then we have optimal algorithm in classical search and the search is constrained to static selection of an element through the deterministic oracle function. Thus, the problem can overcome by introducing dynamic selection of search element. Another drawback of this algorithm is while searching for continuum elements, the Grover's search algorithm might fail for obtaining the solutions with high probability. As it is discussed that quantum computing is the probabilistic model, so obtaining the result cannot be guaranteed with high probability.

References

[1] Dumas J. P., Soni, K, & Rasool A. An Introduction to Quantum Search Algorithm and Its Implementation. In: Advances in Intelligent Systems and Computing – Book Series, 2018, Vol. 808, PP.19–31, (2018)

[2] Eleanor Rieffel and Wolfgang Polak.: An Introduction to Quantum Computing for Non-Physicists. ACM Computing Surveys (CSUR), 300–335, (2000).

[3] Jasmeet Singh and Mohit Singh. Evolution in Quantum Computing. In: 5th International Conference on System Modeling & Advancement in Research Trends, IEEE, 2016.

[4] Ashley Montanaro.: Quantum Algorithms - An Overview Quantum Information, 1-15, (2015).

[5] Kanamori, Y., Yoo S-M Pan, W. D & Sheldon F. T.: A Short Survey on Quantum Computers. International Journal of Computers and Applications 28(3), 227–233, (2006).

[6] Grover, L. K..: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212-219, (1996).

[7] N. David Mermin.: Quantum Computer Science – An Introduction, 1st edn, (2007).

[8] Ramesh, H & Vinay V. String matching in O(n+m) quantum time. Journal of Discrete Algorithms 1(1), 103–110, (2003).

[9] Michael A. Nielsen and Isaac L. Chuang.: Quantum Computation and Quantum Information. 10th Anniversary Edition, Cambridge University Press, UK (2010).

[10] Siddhartha Kasivajhula. Quantum Computing: A Survey. In: Proceedings of the ACM 44th Annual Southeast Regional Conference, pp. 249–253, (2006).

[11] Jozef Gruska. Quantum Computing. Illustrated Edition. McGraw Hill Book Co. Ltd, (2000).

[12] Dan C. Marinescu.: The Promise of Quantum Computing and Quantum Information Theory – Quantum Parallelism (The Abstract Tutorial). In: IEEE 19th (IPDPS'05) International Proceedings on Parallel and Distributed Processing Symposium, IEEE, pp. 112–115, (2005).

[13] Aïmeur, E., Brassard, G. & Gambs, S. Mach Learn 90: 261, (2013)

[14] Ashley Montanaro.: Quantum Pattern Matching Fast on Average, 16-39 (2017).

[15] Jacob biamonte, peter wittek, Nicola pancotti, patrick rebentrost, Nathan wiebe & seth Lloyd. Quantum machine learning, 195-202 (2017)

[16] M. Steffen D. P. DiVincenzo J. M. Chow T. N. Theis M. B. Ketchen.: Quantum computing: An IBM perspective, (2012).

[17] C. G. Almudever, L. Lao, X. Fu, N. Khammassi, I. Ashraf, D. Iorga, S. Varsamopoulos, C. Eichler, A. Wallraff, L.Geck, A. Kruth, J. Knoch, H. Bluhm, K Bertels.: The Engineering Challenges in Quantum Computing, In:Design, Automation & test in europe conference and exhibition, (2017)