Extended Essay Title

Is it feasible for quantum processors to replace the silicon microprocessors used in classical computers of today?

School: Emirates International School – Jumeirah

Session: May 2010

Word Count: 3,838/4,000

Abstract

This extended essay explores the new generation of processing; quantum processors. I chose this topic because it is one of the most up and coming technologies in the computer industry. The research question involves looking at whether silicon microprocessors used today can practically be replaced by quantum processors. Moore's law, one of the most important trends in microprocessor evolution, is going to arrive at a stage where it will break down. Silicon microprocessors will then serve as no use in the advancement of processing speed. At this stage, transistors will be the size of atoms and the laws of quantum mechanics will take effect. Quantum computing can raise hazardous problems for the internet such as compromising its security and communications. This essay has also made use of research papers, books and articles published by physicists, computer scientists and even mathematicians, all of whom are involved in the research and development process of quantum computers. Information of particular mention is a quote from Professor Isaac L. Chuang, leader of IBM Research for quantum computing and a professor at Massachusetts Institute of Technology (MIT). A glimpse was also taken at some of the most powerful quantum algorithms today in addition to a deep physics analysis on the features of a quantum processor. With these resources, the use of logic and reasoning helped conclude whether quantum processors can really replace silicon microprocessors. The investigation suggested that quantum processors will replace silicon microprocessors in the near future because it can execute quantum algorithms much faster done with silicon microprocessors. At the present stage, quantum processors do not serve much use until further research and development has taken place because it can carry out regular algorithms only slightly better than silicon microprocessors.

Word Count: 287/300

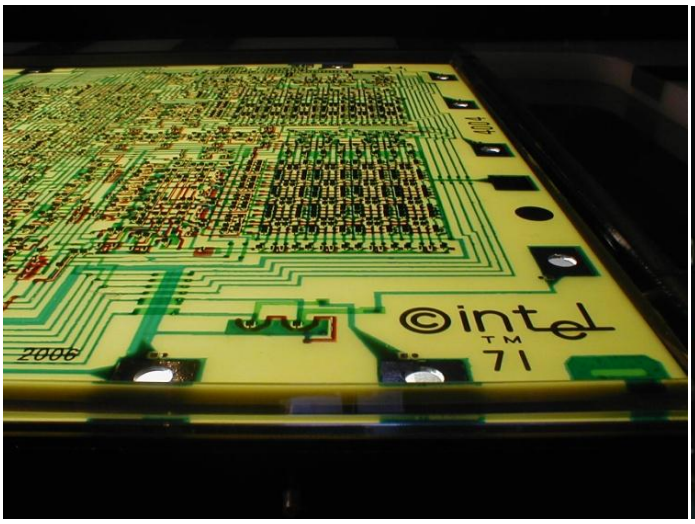
Table of Contents

1. Introduction 4
2. Silicon Microprocessors; The Processor of Today 7
3. The New Age of Processors; Quantum Processors 10
4. Features of Quantum Processors 13
    a. Shor's Algorithm 16
    b. Grover's Algorithm 18
5. Conclusion 21
6. Bibliography 23

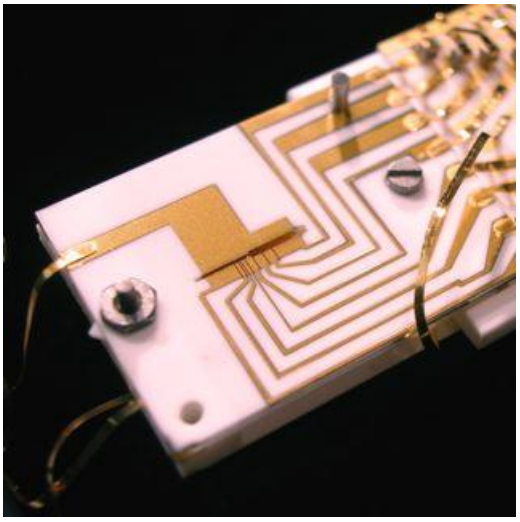
1. Introduction

Gordon Moore is not only the co-founder of the largest silicon chip manufacturing company in the world, Intel, but also the father of Moore's Law, one of the most important trends in Computer Science[1]. Moore's law, or rather his observation of a trend, states that the number of transistors per square inch of integrated circuits will double every 18 months[2,3]. This trend has been very accurate since it came into place in the 1960s as chipmakers have been racing to keep up with the pace of Moore's law in an effort to develop faster, more competitive processors[4].

The modern microprocessor is the most revolutionary invention of mankind. Rapid breakthroughs are continually allowing faster processing speeds to be attained such that the fastest processor five years ago is virtually non-existent and obsolete in the present day market.



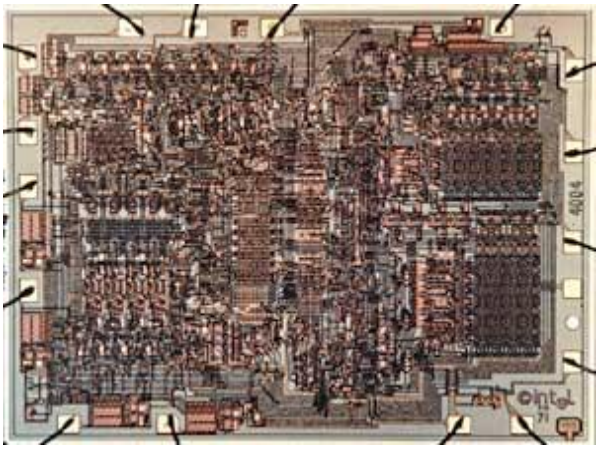
Silicon Microprocessor[5]



Quantum Processor[6]

[1] http://www.pbs.org/transistor/album1/moore/index.html, Retrieved on 7th January 2010, 19:41
[2] http://www.webopedia.com/TERM/M/Moores_Law.html, Retrieved on 7th January 2010, 20:22
[3] "Integrated circuits" are also known as chips or microprocessors.
[4] http://www.ibm.com/developerworks/library/pa-microhist.html, Retrieved on 8th January 2010, 14:07
[5] http://caraudioforumz.com/wp-content/uploads/2008/05/pb120046-1.JPG, Retrieved on 3rd January 2010, 17:52
[6] http://www.scientificamerican.com/media/inline/quantum-computer-nist_1.jpg, Retrieved on 3rd January 2010, 17:50

Microprocessors are referred to as the 'heart' of machines because they control its various processes. The microprocessor of a computer holds the ROM and RAM, which is used to process and store data temporarily. They are necessary for a computer to be able to function because they execute tasks specified by the user and operating system. The first microprocessor, the Intel 4004, was developed in 1971. It could process up to 4 bits at a time so it could only perform simple arithmetic functions such as adding and subtracting[7]. Silicon microprocessors are commonly used today in all electronic devices and are used to regulate the functions of the device. These processors carry out many useful tasks for people today such as file handling, sorting and searching for data as well as executing numerous algorithms whereas regular computer chips are designed to perform a specific function[9]. Nevertheless, as Gordon Moore predicts the inevitable end of his law and any further development of silicon microprocessors, the next logical step is to develop quantum computers[10].



Intel 4004 Microprocessor[8]

"Quantum computing begins where Moore's law ends – about the year 2020, when circuit features are predicted to be the size of atoms and molecules" says Professor Isaac L. Chuang, leader of a group of scientists from IBM Research, Stanford University and University of Calgary[11]. The idea of a quantum computer came from Richard Feynman, a

[7] http://www.howstuffworks.com/microprocessor.htm, Retrieved on 3rd January 2010, 19:04
[8] http://www.ieeeghn.org/wiki/images/d/d3/Intel4004.jpg, Retrieved on 20th January 2010, 17:27
[9] Grant McFarland (2006, Page 2), Microprocessor Design – A Practical Guide from Design Planning to Manufacturing
[10] http://www.howstuffworks.com/quantum-computer.htm, Retrieved on 8th January 2010, 14:32
[11] http://www.pcworld.com/article/18048/ibm_claims_fastest_quantum_computer.html, Retrieved on 8th January 2010, 14:46

Physics Nobel Prize winner, in 1981[12]. As the size of transistors and logic gates on microprocessors decrease over time, they approach sizes at the atomic level where the laws of quantum mechanics come into play[13]. Research in the past on quantum technology has simply been at a theoretical level however, advances in technology over the years have brought us closer to having a complete, working quantum computer[14].

By 2020, it is estimated that the power of silicon in the world will be exhausted so we must find an alternative processor to run computer systems with[15]. The nature of quantum computing makes it a renewable resource because everything in the world is made of atoms. Atoms are a resource that the world will never run out of so it is definitely a long-term solution for the silicon power depletion. This makes quantum computers a viable option to consider when the current technology reaches impenetrable barriers. I chose to explore the technology of quantum processors because of its evidently increasing importance in the future.

This essay will attempt to evaluate and assess whether it is practical to replace silicon processors used in classical computers today with quantum processors.

[12] http://www.faqs.org/patents/app/20090173936, Retrieved on 8th January 2010, 15:00
[13] http://ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm, Retrieved on 5th January 2010, 21:32
[14] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/, Retrieved on 4th January 2010, 14:27
[15] http://www.processor.com/editorial/article.asp?article=articles%2Fp2713%2F39p13%2F39p13.asp, Retrieved on 21st January, 22:59

2. Silicon Microprocessors; The Processor of Today

The microprocessor has rapidly evolved since its creation in 1a971. Before microprocessors were created, computers were controlled by many separate components. As this technology developed, all these individual parts were integrated onto a single piece of silicon, known as a microprocessor[16]. This is the origin of the chip's alternate name, integrated circuits, and has made the microprocessor simpler to recognise. Over the years as Moore's law has progressed, the size of transistors, found on microprocessors have been decreasing, reducing the physical space required in a CPU[17]. This is one of the reasons why the size of computers available on the market are ever decreasing.

As the dimensions of transistors are shrinking, the number that can be placed on a microprocessor has increased over the years. Smaller transistors can switch faster, despite using less current, because they have less capacitance[18]. They use less current which is defined by:

$$I = \frac{Q}{t}$$

This means that they use less charge because charge (Q) is directly proportional to the current (I) as shown by the equation above. Therefore, it takes less charge to move the transistor gate switches 'on' and 'off' which means that processing can occur faster if the same voltage is applied. As a result, it means that Moore's law was derived because of the relationship between the increase in processor speed and the decreasing size of transistors.

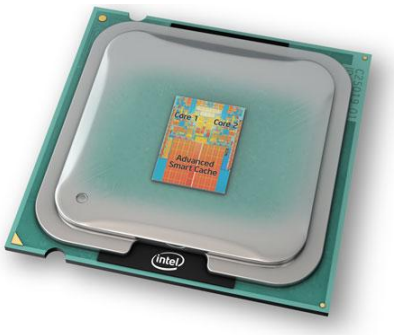
Silicon microprocessors today work using the binary system (0s and 1s). Ones are represented in transmissions by a high pulse of voltage and zeros are represented by a low

[16] Grant McFarland (2006, Page 2), Microprocessor Design – A Practical Guide from Design Planning to Manufacturing
[17] Central Processing Unit (CPU)
[18] Grant McFarland (2006, Page 204), Microprocessor Design – A Practical Guide from Design Planning to Manufacturing

pulse of voltage. The 'on' or 'off' status of a transistor switch on a microprocessor, also, represent 1s and 0s, respectively[19]. Due to this system architecture, there can only be two states that are possible to denote data held in transistors and cables. This is the reason why computers can only process digital data and not in analogue form. Digital-to-Analogue Converters (DAC) and Analogue-to-Digital Converters (ADC) are required for communication so that computers can interpret continuous data. The two states, 'on' or 'off', are also the reason why computers only work with binary code, which has a base of two.

The performance of silicon microprocessors are limited by heat and their circuits. Although the progression of Moore's law is allowing for faster processors, the amount of heat produced in a compressed area is also increasing because of smaller transistors[20]. The excessive heat can damage the device or reduce CPU performance so the heat is transferred away from the microprocessor through heat conduction, convection and radiation. The use of cold sinks and fans aid in transferring heat away from the transistors[21]. This is important so that the life of microprocessors are extended as long as possible.

There have been many recent developments in microprocessor architecture. Silicon microprocessors used today have undergone major changes such as multi-core technology. A regular single-core processor is limited by the speed of data transferred across the system bus because it has to wait for devices slower than itself to respond and process. The cores in multi-core processors handle incoming data strings simultaneously to improve efficiency. The main task that these processors are developed for



Multi-Core Processor[22]

[19] Mohamed Rafiquzzaman (2008, Page 1), Microprocessor Theory and Applications with 68000/68020 and Pentium
[20] http://news.cnet.com/2009-1001-275823.html, Retrieved on 23rd January 2010, 17:13
[21] http://www.electronics-manufacturers.com/info/circuits-and-processors/microprocessor.html, Retrieved on 23rd January 2010, 18:08
[22] http://www.xbitlabs.com/images/cpu/intel-wolfdale/c2d-inside.jpg, Retrieved on 2nd February 2010, 16:44

is multi-tasking[23]. This is very useful to carry out system processes in the background as well as user-defined processes such as running a virus scan and using Adobe Photoshop at the same time. This design allows more processes to be executed in a shorter timeframe. Multi-core processors are also faster, use less power, are smaller in size and cheaper to manufacture[24]. An example of a multi-core processor would be the Intel Pentium Core 2 Duo, a dual-core processor.

[23] http://www.wisegeek.com/what-is-a-dual-core-processor.htm, Retrieved on 25th January 2010, 20:54
[24] http://www.wired.com/science/discoveries/news/2006/07/71467, Retrieved on 25th January 2010, 21:43

3. The New Age of Processors; Quantum Processors

Quantum processors are currently a development in the making. Computer scientists and researchers at leading institutes around the world are exploring the concept of creating a quantum computer. The quantum processor is based on the use of atoms rather than circuits and chips. A quantum processor requires individual atoms to be isolated and the theory of a quantum dot determines the data stored in each atom. A quantum dot is a single electron trapped inside a cage of atoms. When this electron is exposed to a laser for a certain duration and at a specific wavelength, the electron becomes excited. If the laser is applied again with the same conditions, the electron becomes grounded. This is used to represent data in quantum computing where the excited electron is a 1 and the grounded electron is a 0[25]. Quantum processors are based on quantum bits, also known as qubits, rather than regular bits. The binary digit system involves the use of 0s and 1s where a bit is either 0 or 1[26]. However, the qubit system for quantum processors can allow a qubit to be a superposition of 0 and 1 at the same time[27]. This is represented as:

$$|\phi = \alpha|0 + \beta|1$$

The 'α' and 'β' are complex numbers such that the numbers are in the form $z = x + iy$ where $i = \sqrt{-1}$. The laws of quantum mechanics state that the modulus squared of the imaginary parts of the equation returns the probability that the qubit is a '0' or a '1'.

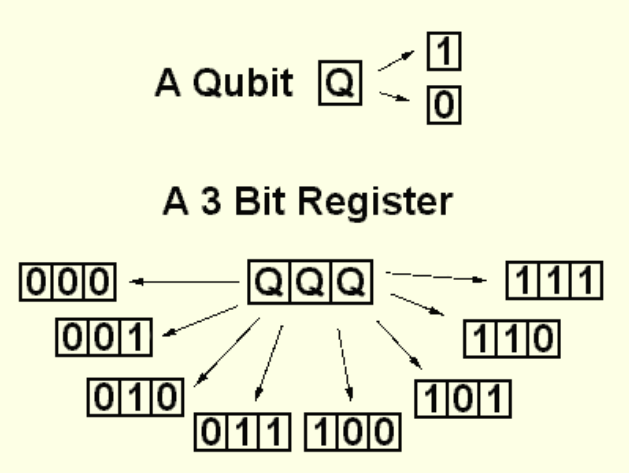
$|\alpha|^2$: Tells us the probability of finding $|\phi$ in state $|0$
$|\beta|^2$: Tells us the probability of finding $|\phi$ in state $|1$ [28]

[25] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/#9.2, Retrieved on 2nd February 2010, 14:45
[26] 'Binary digit' is the full form of 'bit'.
[27] http://www.youtube.com/watch?v=DNatzhe4BoQ, Retrieved on 4th January 2010, 16:44
[28] David McMahon (2008, Page 12), Quantum Computing Explained

This method of representation makes quantum processors very different from the silicon processors we use today.

In order for quantum processors to execute methods, the qubits require a quantum bus to communicate with each other. A quantum bus is a wire, which transmits photons containing information from one qubit to another[29]. At present, several models of quantum processors have been created. The first two-qubit quantum processor was created by researchers at Yale University in June 2009. It can execute a basic search and very simple quantum tasks. They made the two qubits with a billion aluminium atoms, which acted like single atoms that could occupy two different energy states[30]. This is similar to the two states possible on silicon microprocessor transistors and it means that quantum computers will only be able to process data in digital format like classical computers today.

Quantum computers work using quantum registers. This is a group of qubits and like a regular register, can represent 2^n different values. A quantum register is used to transform quantum algorithms into a state such that there will be a high probability of obtaining the correct value[31]. This element of a quantum computer system is vital to the success of quantum technology. A quantum register, in contrast with regular registers, "can store an exponential amount of information"[32].



Quantum Register[33]

[29] http://www.tgdaily.com/hardware-features/43017-first-quantum-processor-created, Retrieved on 2nd February 2010, 23:56
[30] Ibid.
[31] http://alumni.imsa.edu/~matth/quant/473/473proj/node6.html, Retrieved on 2nd February 2010, 13:40
[32] Ibid.
[33] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/, Retrieved on 2nd February 2010, 15:54

The diagram on the previous page demonstrates how processes are handled by a quantum register. A process executed on one set of qubits would execute each and every possibility, in parallel with each other, as though in separate universes[34].

The world record quantum computation is "3 × 5 = 15" which was performed by a quantum processor at IBM[35]. The processor can only perform such a small calculation because the qubits, used in the process, can only be isolated for a microsecond before they escape[36].

[34] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/, Retrieved on 2nd February 2010, 15:54
[35] http://www.youtube.com/watch?v=5W4e7ZE0Nv0&feature=related, Retrieved on 21st January 2010, 22:35
[36] http://www.tgdaily.com/hardware-features/43017-first-quantum-processor-created, Retrieved on 26th January 2010, 21:46

4. Features of Quantum Processors

Quantum computers have many strong qualities that must be taken into consideration for its feasibility. The atomic property of superposition is an advantage for quantum processors because it can allow a bit to be 0 and 1 simultaneously. When quantum registers perform computations on data, each part of the superposition is processed. This concept is also known as quantum parallelism and the ability to do this allows quantum processors to carry out several processes at the same time[37]. This is similar to parallel processing or dual-core processing, where two processors or cores perform two separate tasks, except in the quantum processor's case, there is only one sole processor that carries out the tasks simultaneously[38].

The superposition property opens up endless possibilities in terms of capacity. Since individual atoms are used to store data and there are more than a million atoms in a mere full stop, storage capacities can arrive at new fronts with quantum processing. Yottabytes of capacity may be achievable so today's nightmare of reaching full hard drive capacity could simply be history in the quantum computing age. This is because even all the information on the Internet is approximately 500 exabytes of storage capacity[39,40]. The same theory can be related to the processing power of quantum computers. Quantum processors can be supplied with countless atoms which could make the raw processing power of a quantum computer far greater than the silicon microprocessors in use today.

Quantum processors would theoretically be affected by heat in the same way as silicon microprocessors would be. Since the atoms in the processor vibrate, they have kinetic energy which is defined by:

---

[37] http://alumni.imsa.edu/~matth/quant/473/473proj/node6.html, Retrieved on 2nd February 2010, 14:30
[38] http://www.youtube.com/watch?v=P7PkPrbNdx4, Retrieved on 4th January, 18:30
[39] http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion, Retrieved on 4th January 2010, 18:45. Although this article is slightly old (May 18th 2009), an extrapolation of the Internet's growth would probably result in the Internet's current size being above 500EB but less than 1ZB.
[40] 1,024 exabytes = 1 zettabyte, 1,024 zettabytes = 1 yottabyte

$$KE = {}^{1}/_{2}\ mv^2$$

The average kinetic energy of a molecule is directly proportional to its temperature.

$$KE\ \alpha\ T$$

With the massive amount of atoms, being used as qubits, that vibrate in synchronisation, large amounts of heat will be emitted. The surrounding area of the computer system will act as a cold sink and this will increase its temperature. This can pose serious problems such as damage to peripherals connected to the quantum system because of excessive heat produced. Another problem that this could cause is damage to the health of quantum computer users. Excessive exposure to heat, especially with direct physical contact, can damage nerves in the hands as well as other parts because of strained exposure. In addition, if heat is applied to the system, it can increase the kinetic energy of the system unevenly and cause the vibration of atoms to fall out of synchronisation. This would ruin the calculation as the data stored in the atoms would be completely altered and no data recovery possible. Silicon microprocessors are also negatively affected by heat, which means that they both have a common weakness. This will have to be resolved by using laws of thermodynamics to transfer or simply reduce the heat given out.

Quantum computers are very vulnerable to forms of interference. Since atoms are the base of quantum processing, they must be preserved and protected in order to retain stored data. This major principle is called coherence where the integrity of the data stored is not disturbed. The atoms in use are prone to waves such as cosmic rays from outer space, radiation and even movement nearby[41]. This can distort the vibrations of the atoms and cause errors in calculations. This problem will have to be mastered by creating a protective container for quantum processors that do not vibrate. This can prove to be an enormously

[41] http://www.youtube.com/watch?v=5W4e7ZE0Nv0&feature=related, Retrieved on 4th January 2010, 21:10

difficult task. This protective casing would also be required to use quantum computers in outer space where there is no atmosphere protection from the sun's rays[42].

Since the physical component of quantum computing is so different from classical computers today, it raises different issues. Atoms holding the data must be preserved because a crack or damage to the container can be disastrous. Data will be permanently lost if the atoms escape or the controlled vibrations are altered. Silicon microprocessors, in contrast, store data according to the state of the transistor switches. Another problem related to this is the seclusion of atoms to be used with quantum processors. The process of doing this is very expensive and very difficult as atoms can only be trapped for a very short time. One of the reasons for this is because lasers used on quantum dots only excite electrons for less than a second so there is a limit on quantum algorithms that can be executed[43]. An issue that comes to light, also, is the storage of data in quantum computers. If the vibration of atoms are used to store data in a non-ideal/real world, inelastic collisions between molecules mean that kinetic energy is degraded to heat energy. The kinetic energy of the system would then decrease and data held in atoms altered. Therefore, the casing used to hold atoms must also be able to maintain the exact amount of vibrations of atoms.

In addition, quantum processors can be used for modelling complex quantum processes. This is very useful to view the various outcomes that could occur from performing certain actions as well as for manipulating variables in a simulated situation, such as testing how a new drug acts on faulty biochemistry[44]. Although silicon microprocessors are capable of doing the same, they have certain barriers. Quantum processors can simulate more intricate processes and include the smaller, finer details of a simulation that microprocessors cannot.

[42] http://www.youtube.com/watch?v=5W4e7ZE0Nv0&feature=related, Retrieved on 4th January 2010, 21:10
[43] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/#9.2, Retrieved on 2nd February 2010, 16:51
[44] http://www.youtube.com/watch?v=P7PkPrbNdx4, Retrieved on 21st January 2010, 23:24

A strong advantage of quantum processors are that they are able to execute quantum algorithms. These algorithms can only be executed efficiently on quantum computers[45]. In the next section, I will discuss two of the most important quantum algorithms at the present time, Shor's and Grover's.

a. Shor's Algorithm

One of the major features of quantum processing involves Shor's algorithm. This algorithm is used to decode RSA, which is the common encryption code used to protect data on the Internet. The RSA decryption technique requires finding the prime factors of very large numbers. Shor's algorithm cannot be feasibly carried out by the 'classical' computers of today so it is thought to be 'uncrackable'[46,47]. For this reason, RSA encryption is used by government agencies and private individuals to protect their data[48]. However, quantum computers will be able to execute this algorithm much faster than classical computers. This poses the problem that information on the Internet becomes no longer secure and it raises concerns for Internet users all over the world. Regardless of this, the latest technology of quantum processing could possibly introduce a newer and more powerful form of encryption in compensation for outdating RSA, quantum cryptography. The following pseudo code demonstrates Shor's algorithm.

```
Input: odd integer N
Repeat
Randomly select x∈ {2,. . . ,N − 1} a ∈ {2,. . . ,N∨1}
d = gcd (x,N)
If d≥2 Then u = d, v = N/d
Else
Find the order r such that xr = 1 mod N
```

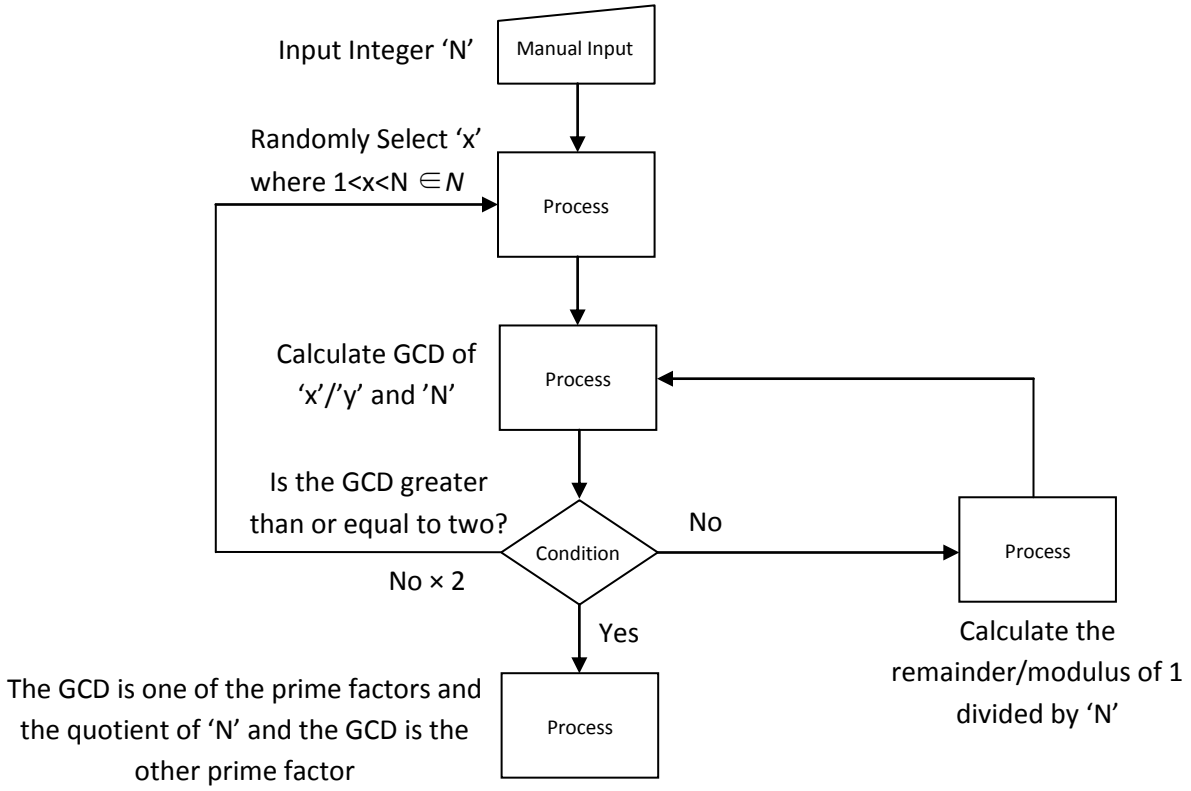
[45] http://web.mit.edu/newsoffice/2009/quantum-algorithm.html, Retrieved on 3rd February 2010, 00:43
[46] 'Classical' is a reference to the computers that are used worldwide today based on silicon microprocessor technology.
[47] 'Uncrackable' means that it is impossible for hackers to execute the algorithm and break the code.
[48] http://www.cs.rice.edu/~taha/teaching/05F/210/news/2005_09_16.htm, Retrieved on 4th January 2010, 18:09

```
y = xr/2 −1 mod N
d = gcd (y,N)
If d≥2 Then u = d, v = N/d
          Until find u,v
```
[49]

Shor's algorithm requires the prime factors of large numbers, typically one hundred digits long, to be calculated. The algorithm requests for an odd integer, 'N', to be input because only odd numbers can be prime numbers with the exception of two which is far too simple to calculate; all even numbers are divisible by two. A random number is selected between two and 'N'. The Greatest Common Divisor (GCD) of this random number and the prime number input is calculated[50]. If the GCD, which is assigned to 'd', is greater than or equal to two, then the procedure is complete and this GCD is assigned to a variable. Half of the prime number input is calculated and is assigned to a second variable and the algorithm terminates. However if the GCD is less than two, then the randomly selected number is multiplied by 'r'. This is then divided by two minus one modulus of the prime number. The GCD of this and the prime number input is calculated. If the result is greater than or equal to two, the same variables are created and assigned as before. Otherwise, the entire procedure is repeated until the variables are found. The system flowchart below demonstrates the execution of Shor's algorithm.

[49] David McMahon (2008, Page 218), Quantum Computing Explained, from the Notes of Professor John Watrous of the University of Waterloo, Canada

[50] GCD is also known as the Highest Common Factor (HCF)



The BigO Efficiency of Shor's Algorithm for quantum computers is $O(\log_3(n))$. The BigO Efficiency of Shor's Algorithm for the computers used today is O(poly(n)). The polynomial time in the BigO notation means that this algorithm cannot be executed in a feasible time span (billions of years) with the computers we use today. This is because as the size of 'N' increases, the number of steps required to execute the algorithm exponentially increases. However due to the superpositioning capability of qubits, Shor's algorithm could be executed and the RSA cracked in a matter of days or weeks depending on the running time coefficients of the quantum processor[51].

b. Grover's Algorithm

Grover's algorithm is another quantum algorithm, invented by Lov Grover in 1996. This is another important feature of quantum computing. It is used to search unsorted

[51] Marco Lanzagorta and Jeffrey Uhlmann (2009, Page 92), Quantum Computer Science

databases[52]. The following pseudo code algorithm demonstrates the steps taken in the execution of Grover's algorithm.

1. Initialise the quantum computer to be an equal superposition of all possible N states.
2. Repeat the following steps O($\sqrt{N}$) times:

(a) Let the system be in any state. Evaluate the search function at that state. If it evaluates to 1, then phase rotate by π radians. Otherwise, do not change the system.

(b) Apply the diffusion transform. Create a diffusion transform matrix with $D_{ij} = \frac{2}{N}$ if $i \neq j$ and $D_{ii} = -1 + \frac{2}{N}$ otherwise.

3. Finally, measure the system to get the desired state with probability greater than ½ [53]

The BigO efficiency of a regular linear search algorithm is O(n). Grover's algorithm's BigO efficiency is O($\sqrt{n}$) showing that in large databases or lists, searches with Grover's algorithm are 'quadratically' faster[54,55]. Grover's algorithm also uses O(log n) storage space as Shor's algorithm does[56]. It has a high probability of success and the probability of failure is reduced every time the algorithm is repeated.

When a search with Grover's algorithm is performed on a database that has 100 records, a quantum computer would only need to make 10 searches to find the record needed. If the size of the database increases, the time taken for a regular computer to find a record would increase rapidly. On the other hand, the effect that it has on quantum computers is negligible[57]. This means that using large information systems will become more efficient with these type of quantum algorithms.

[52] http://www.knowledgerush.com/kr/encyclopedia/Grover's_algorithm/, Retrieved on 21st January 2010, 19:46
[53] http://www.cs.indiana.edu/~mewhiteh/files/quantum_genetic_search.pdf, Retrieved on 2nd February 2010, 19:50
[54] http://www.katzgraber.org/teaching/FS08/files/solca.pdf, Retrieved on 21st January 2010, 19:44
[55] 'Quadratically' means of the exponential power two (squared).
[56] http://kastor1337.info/EPITA/Quantum%20Computing.pdf, Retrieved on 2nd February 2010, 18:54
[57] http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/#4.2 Grover's algorithm, Retrieved on 3rd February 2010, 09:12

	Shor's	**Grover's**
Silicon Microprocessor	O(poly(n))	O(poly(n))
Quantum Processor Execution	$O(\log_3(n))$	$O(n^{1/2})$
Quantum Processor Storage Space	O(log(n))	O(log(n))

[58]

The table above clearly demonstrates the difference between quantum algorithms. As can be seen, quantum algorithms cannot be practically run on classical computers today because their efficiency renders them in polynomial time. The efficiency of execution of both Shor's and Grover's algorithms exemplifies the power and potential of quantum processors. Quantum processor storage space has also decreased compared to that of silicon microprocessors which have standard efficiency. Less space occupied in the memory means more processes that can be carried out together.

[58] Ibid. Information collated from previous footnote (Ibid) as well as from the two sub-sections before.

5. Conclusion

It is unlikely that the first quantum processor will be able to compete with the speed of the silicon microprocessors available in 2025 as Moore's law continues to progress to its end[59].

One of the main concerns of new technology is the security issues and vulnerabilities it poses to confidential and personal data. Quantum cryptography would have to be developed and implemented before quantum technology could be made public. The accuracy and reliability of processed data is also a very important element in developing new technology. Protective casing for atomic modules would also have to utilised for coherence of processing. This is one of the main weaknesses of quantum processors that have to be dealt with.

Quantum processors are able to execute quantum algorithms such as Shor's and Grover's algorithm. The difference in BigO notation between certain algorithms implemented on silicon microprocessors and quantum processors is very large and provides a strong advantage to the latter. The speed of quantum and silicon microprocessors is very similar so quantum processors do not offer an overall advantage to future users in reference to regular algorithms. This is simply a problem at present because quantum processors are specially catered to carrying out quantum algorithms. Since few quantum algorithms have been designed, quantum processors may not be valued as much as they would be in the future when more beneficial quantum algorithms have been devised.

Quantum processors offer numerous advantages for the future. It promises to be allow more efficient algorithms to be executed, bring stronger security systems and greater capabilities. On the other hand, lots of research and development still need to take place

[59] Marco Lanzagorta and Jeffrey Uhlmann (2009, Page 30), Quantum Computer Science

before quantum computers can be sold to the general public. Once the appropriate research has been carried out and appropriate safety measures taken, quantum processors can offer the world the next generation of processing when the era of silicon microprocessors comes to an end.

Bibliography

Lanzagorta, Marco and Uhlmann, Jeffrey (2009), *Quantum Computer Science*; Morgan & Claypool Publishers; Columbia, Missouri (USA)

McMahon, David (2008), *Quantum Computing Explained*; John Wiley & Sons, Inc.; Hoboken, New Jersey (USA)

McFarland, Grant (2006), *Microprocessor Design – A Practical Guide from Design Planning to Manufacturing*; McGraw-Hill Publishing Companies; USA

Rafiquzzaman, Mohamed (2008), *Microprocessor Theory and Applications with 68000/68020 and Pentium*; John Wiley & Sons, Inc.; Hoboken, New Jersey (USA)

Bone, Simon & Castro, Marias; A Brief History of Quantum Computing, http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/, Retrieved on 4th January 2010, 14:27

Bonsor, Kevin & Strickland, Jonathan; How Quantum Computers Work, http://www.howstuffworks.com/quantum-computer.htm, Retrieved on 8th January 2010, 14:32

Brain, Marshall; How Microprocessors Work, http://www.howstuffworks.com/microprocessor.htm, Retrieved on 3rd January 2010, 19:04

Chidi, Jr., George A.; IBM Claims Fastest Quantum Computer, http://www.pcworld.com/article/18048/ibm_claims_fastest_quantum_computer.html, Retrieved on 8th January 2010, 14:46

CNN – Quantum Computers, (Documentary) http://www.youtube.com/watch?v=DNatzhe4BoQ, Retrieved on 4th January 2010, 16:44

Grover's algorithm, http://www.knowledgerush.com/kr/encyclopedia/Grover's_algorithm/, Retrieved on 21st January 2010, 19:46

Gordon Moore, American Institute of Physics & ScienCentral Inc; http://www.pbs.org/transistor/album1/moore/index.html, Retrieved on 7th January 2010, 19:41

Great moments in microprocessor history (2004), http://www.ibm.com/developerworks/library/pa-microhist.html, Retrieved on 8th January 2010, 14:07

Hardesty, Larry; MIT News Office; Quantum computing may actually be useful, http://web.mit.edu/newsoffice/2009/quantum-algorithm.html, Retrieved on 3rd February 2010, 00:43

Hayward, Matthew; The Quantum Register, http://alumni.imsa.edu/~matth/quant/473/473proj/node6.html, Retrieved on 2nd February 2010, 14:30

Kanellos, Michael; Little Package, Big Changes; Big changes ahead for microprocessors http://news.cnet.com/2009-1001-275823.html, Retrieved on 23rd January 2010, 17:13

Kayne, R.; What is a Dual Core Processor, http://www.wisegeek.com/what-is-a-dual-core-processor.htm, Retrieved on 25th January 2010, 20:54

Lene Hau & Quantum processing, (Documentary at Harvard & MIT) http://www.youtube.com/watch?v=P7PkPrbNdx4, Retrieved on 4th January 2010, 18:30

Michio Kaku on Quantum Computing, (Interview) http://www.youtube.com/watch?v=5W4e7ZE0Nv0&feature=related, Retrieved on 21st January 2010, 22:35

Microprocessor, http://www.electronics-manufacturers.com/info/circuits-and-processors/microprocessor.html, Retrieved on 23rd January 2010, 18:08

Milchman, Eli; Intel Dual-Core FAQ, http://www.wired.com/science/discoveries/news/2006/07/71467, Retrieved on 25th January 2010, 21:43

Moore's Law, http://www.webopedia.com/TERM/M/Moores_Law.html, Retrieved on 7th January 2010, 20:22

Parodi, F. & Wacrenier, V.; Quantic Computing; A travel into qubits... http://kastor1337.info/EPITA/Quantum%20Computing.pdf, Retrieved on 2nd February 2010, 18:54

Quantum Computers, http://ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm, Retrieved on 5th January 2010, 21:32

Solca, Raffaele; Grover's algorithm, http://www.katzgraber.org/teaching/FS08/files/solca.pdf, Retrieved on 21st January 2010, 19:44

Takahashi, Dean; Life After Moore's Law; Law Will Come To An End, But Alternatives To Silicon Chips Are Slow Coming, http://www.processor.com/editorial/article.asp?article=articles%2Fp2713%2F39p13%2F39p13.asp, Retrieved on 21st January 2010, 22:59

West, Jacon; The Quantum Computer, http://www.cs.rice.edu/~taha/teaching/05F/210/news/2005_09_16.htm, Retrieved on 4th January 2010, 18:09

Whitehead, Matthew; Using Grover's algorithm for Genetic Search, http://www.cs.indiana.edu/~mewhiteh/files/quantum_genetic_search.pdf, Retrieved on 2nd February 2010, 19:50

Woollacott, Emma; First quantum processor created, http://www.tgdaily.com/hardware-features/43017-first-quantum-processor-created, Retrieved on 4th January 2010, 23:31

Wray, Richard; Internet data heads for 500bn gigabytes, http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion, Retrieved on 4th January 2010, 18:45

http://caraudioforumz.com/wp-content/uploads/2008/05/pb120046-1.JPG, Retrieved on 3rd January 2010, 17:52

http://www.ieeeghn.org/wiki/images/d/d3/Intel4004.jpg, Retrieved on 20th January 2010, 17:27

http://www.faqs.org/patents/app/20090173936, Retrieved on 8th January 2010, 15:00

http://www.scientificamerican.com/media/inline/quantum-computer-nist_1.jpg, Retrieved on 3rd January 2010, 17:50

http://www.xbitlabs.com/images/cpu/intel-wolfdale/c2d-inside.jpg, Retrieved on 2nd February 2010, 16:44