A perspective on the Development of Quantum Computers and the Security challenges

Laith R. Fleih, Abdullah Abdulabbas Nahi Alrabeeah, Khalid Fadhil jasim
College of science, Department of Computer Science, Cihan University – Erbil, Kurdistan Region, Iraq

Abstract

The amount of data produced and processed every day is increasing exponentially, and reaching unthinkable levels. This amount of data has to be stored and processed by something. While the conventional computers are reaching their limits in data storage and processing, and this dictates the need for a nano sized transistors. Quantum computers can provide genius solution for that issue. Quantum computing is an emerging interdisciplinary field in information technology. This technology acquired its name, because it is based on quantum physics. In this article we present a new perspective on the progress in the research efforts on quantum computing technology and their likelihood to replace the conventional computers and change the way we manipulate data and information. Also we claim this might be the first article in the region tackling quantum technology.

Keywords: Development of Quantum, Quantum Computers, Security challenges, Computers.

1- Introduction

In this modern world we live in, which is rightly called the age of knowledge and technology revolution, extremely large amount of data are produced daily, and it is increasing exponentially. The massive amount of processing power provided by conventional digital computers will soon reach their limits in storage capacity and data processing capabilities. Also the transistor size of the conventional digital computers is reaching the nano subatomic level, accordingly the conventional Newtonian physics will collapse and the quantum phenomena will manifest itself [1]. Therefore scientist and engineers strive to develop new technology which can efficiently handle the future needs for storage capacity and processing speeds of the incredibly huge amount of data, and the complexity of large systems and calculations especially in application areas such as cryptography, biotechnology, simulation, …etc.

DOI: http://doi.org/10.24086/cocos2022/paper.754
searching. People naturally ask if they can continue to delay acting, since there are many additional serious and important matters at hand. Whether one can continue to delay approximately depends on three questions. First, how long do you need your cryptographic keys to be remain secure? Denote this number by x, the security shelf life. We may have x 5 0 years for applications requiring only real-time security. Or maybe x 5 10, 20, 100 years when protecting your personal condition info, trade secrets, or national security info. The value of x is in common a individual or business or strategy decision. Next, how lengthy will it take to deploy a set of tools that are quantum safe? Denote this number by y, the migration period. For example, we may have y 5 0 years if this is only a matter of implementing an auto-update that replaces AES-128 with AES-256 within a system fully controlled by a single vendor. Though, we may have y 15 years if it involves a relatively untested public-key encryption method that must be adapted for a constrained environment with many players who must agree on a standard. Last, how long will it be prior to a quantum computer, or some other technique, breaks the currently deployed public-key cryptography tools? Let z denote this amount, the collapse time[13].

2- The Quantum Physics

A basic understanding of quantum physics is necessary to understand how quantum computers work, as well as to help comprehend their limitations and the inherited difficulties in constructing them. Quantum physics is concerned with studying matter and energy at subatomic levels. The behavior of these elementary particles is random and uncertain, and it is not possible to simultaneously measure more than one feature of these particles for example both the position and momentum of these particles cannot be measured simultaneously. Also, quantum theory assumes that energy is not continuous but it comes in small discreet units known as quanta. The two relevant aspects of quantum theory to quantum computing are the phenomena of superposition and entanglement.

2.1- Superposition

Can be explained through an example of an electron in a magnetic field and completely isolated from any other influences; the electron will spin either with the magnetic field or opposite to the magnetic field. Assuming we apply a pulse of energy such as a one unit of laser energy this will change the electron spin from one state to another, but, what if we apply half a unit of laser energy at the particle? According to the quantum theory the particle will enter the superposition states and behaves as if it is in both states simultaneously [2].

2.2-Entanglement

This is the correlation between particles such as electrons or photons which have been interacted in some point and they retain a relation among them and they become entangled with each other as pairs even when they are separated by thousands of kilometers, therefore knowing the spin state of a particle makes one to know the spin state of the entangled particle in the opposite direction no matter how great is the distance between the entangled particles. Also due to superposition the measured particle has no single spin direction before being measured but it is in both spin states simultaneously [2].

3- The quantum Computers

In contrast to conventional digital computers which implement binary digits or bits with values 0 or 1 in its data processing tasks, quantum computers uses what is called qubits which can be generated using the quantum states of elementary particles instead of using electronic gates made of transistors to represent 0 or 1, by switching On and Off.

![Figure 1 An image of the D-wave quantum processor.](http://doi.org/10.24086/cocos2022/paper.754)
of a qubit it will collapse to either 0 or 1, as anticipated from the laws of quantum physics. A mean implementation of a qubit could use the two energy levels of an atom.

![Classical Bit vs Quantum Bit](image)

Figure 2 The representation of Classical Bit versus Quantum Bit

A ground state representing \(|0\rangle\), and

An excited state representing \(|1\rangle\)

By using superposition to represent data, a single qubit can be forced into a superposition of the two states denoted by the addition of the state vectors:

\[
|\psi\rangle = \alpha_1 |0\rangle + \alpha_2 |1\rangle
\]

Where \(\alpha_1\) and \(\alpha_2\) are complex numbers and represent the probability of the superposition collapsing to \(|0\rangle\) or to \(|1\rangle\). The \(\alpha\)'s are called probability amplitudes.

In a balanced superposition, \(\alpha = 1/\sqrt{2^n}\) where \(n\) is the number of qubits.

\[|\psi\rangle = |000\rangle + \frac{1}{\sqrt{8}} |001\rangle + \ldots + \frac{1}{\sqrt{8}} |111\rangle\]

Therefore, with three qubits of data, a quantum computer can store all eight patterns of 0 and 1 concurrently. That means a three-qubit quantum computer could calculate eight times faster than a three-bit digital computer. And for comparison, typical personal computers today calculate 64 bits of data at a time. A quantum computer with 64 qubits would be 2 to the 64th power faster or about 18 billion billion times faster [3].

4-New trends and achievements in Quantum Computer research

In this section we represent the resent development in quantum hardware and software, and emphasizing the challenges of facing the developers in their effort to make the quantum technology a reality.

4.1- Quantum hardware

Recently Google and NASA teamed up to share the world first commercial quantum computers manufactured by Canada’s D-wave systems, with estimated cost of about $10 million US. The chips of this computer have to be maintained in extremely cold temperature near absolute zero to operate. Google is using this computer which is based at Google’s Quantum Artificial Intelligence Lab to study what is called Glass problem figuring out if users are blinking on purpose or involuntarily[4]. Also early adopters of D-Wave machines include Lockheed Martin, and the University of Southern California. However, a vigorous controversy surfaced among quantum computation researchers about the D-Wave machine as noted by Erica Klarreich in here article entitled “Is That Quantum Computer for Real? There May Finally Be a Test” published in Quanta Magazine in 23 August 2013. The researchers question the claimed abilities of the D-Wave machine such as speed and whether it is really implementing the counterintuitive weirdness of quantum physics [5].

In the meantime other researchers are coming up with new ideas and products to perfecting this emerging technology. In their paper entitled, “Integrated spatial multiplexing of heralded single-photon sources, Collins and his coworkers gave a description of a microchip they have been able to develop which can produce photons on demand. Photons are light particles which can readily carry quantum information, and this has application in quantum technology such as quantum computers and quantum communication. This microchip could be a

DOI: http://doi.org/10.24086/cocos2022/paper.754
breakthrough development because it can produce single photon at a time and that opposes the gregarious nature of photons, which they like to appear as group [6].

The applied physics group at the University of Geneva, Switzerland, have been able to produce Crystal Quantum Memories based on quantum entanglement [5].

Working on quantum repeaters a consortium of researchers from four European countries (France, Germany, Sweden and Switzerland) with a finance resource of 1.9 million Euro from the European Commission have taken a major step forward in quantum technology by introducing 'Quantum repeaters for long distance fiber-based quantum communication' (QUREP) which will make quantum communication and computing commercially available in the next ten years [5].

In 13 September 2013, Tiffany Trader published an article in the HPCWire web site entitled Quantum Computing for Everyone in which she predicted that quantum computing will soon be available for anyone with Web browser through which they can access the primitive form of this powerful technology. The article also emphasizes the concern of scientists in Bristol University about the limited access to this technology, available to very few researchers, and they believe that quantum technology should be available to all scientists globally, accordingly and as the 20th of September 2013, the quantum photonic processor housed at the Centre for Quantum Photonics at the University of Bristol became available to scientists and researchers everywhere through the Internet, opening the door for quantum cloud computing or the Qcloud.

A major issue facing the development of quantum computer is the complexity of the quantum circuitry needed to carry out the elementary logic operations. The majority of quantum algorithms are based on controlled operations which are realized by decomposing them into the elementary logic gate set. This decomposition adds complexity. To produce small scale quantum circuits. Dr. Xiao-Qi Zhou and his colleagues at the university of Bristol’s Center for Quantum Photonics and the University of Queensland, Australia, have shown a completely new solution to tackle this problem by using an extra degree of freedom of quantum particles, and they have constructed several controlled operations using this method, this will significantly reduce the complexity of the circuitry for quantum computer [7].

Another step along the road for quantum computing comes from Germany where Janik Wolters and his team of researchers at Humboldt Universität in Berlin, succeeded in building an elementary hybrid form of quantum computer using electronic excitations in nano-diamonds as qubits and optical nanostructures, so-called photonic crystals with tailored optical properties. Their results could be a strategy for scaling up a large scale quantum systems [8].

4.2- Quantum Software

In the previous section we reviewed the advances in the hardware of quantum computing or leading to make quantum computing a reality. On the other hand, there has not been such progress in quantum software because software developers don’t have the hardware to develop the software needed to run that hardware, until a quantum computer became available even in its primitive form. However, some scientist proposed some algorithms which can be used to run quantum computers such as Work on quantum software gained momentum with developing a machine language and operating system to make the hardware usable and useful. In 2009 Matthew Daniel Purkeypile In his Ph.D. thesis proposed a framework named COVE for developing software to run quantum computers. The following diagram shows where Cove and other proposals fit into the various levels of programming ranging from the hardware at the bottom, which is the machine language to an application software at the top. Therefore users will not be aware they are using a quantum computer.

![Figure 3. Abstraction Levels targeted by Cove.](http://doi.org/10.24086/cocos2022/paper.754)
SAOI, is the Server Application Programming Interface. This is the machine code which represents the low level settings of the qubit units of the D-wave quantum computer. The code is housed in remote server and by using a web interface, and a local webserver parses the incoming requests and queues and sorts codes automatically. The adaptation of this web based system allows multiusers to use the system simultaneously [9, 10].

5- Quantum computer versus traditional digital computer

In the following table we present a comparison between some features of quantum computer and conventional digital computer.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Quantum Computer</th>
<th>Digital Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Can solve extremely large and complicated tasks</td>
<td>Limited</td>
</tr>
<tr>
<td>Operational Principle</td>
<td>Data and operations are based on subatomic quantum properties “Qubits”</td>
<td>Data and operations are based on binary digits system “Bits”</td>
</tr>
<tr>
<td>Development</td>
<td>Is still in its infancy</td>
<td>Almost at its theoretical limit</td>
</tr>
<tr>
<td>Speed</td>
<td>Millions of times faster than a supercomputer</td>
<td>Limited speed</td>
</tr>
<tr>
<td>Basic components</td>
<td>Elementary particles such as photons or electrons.</td>
<td>Transistors, electronic gates</td>
</tr>
<tr>
<td>Operations results</td>
<td>Difficult to verify</td>
<td>Verifiable</td>
</tr>
<tr>
<td>Operating systems</td>
<td>Internet based</td>
<td>Built in</td>
</tr>
<tr>
<td>Software</td>
<td>Equivalent to parallel processing [12]</td>
<td>Mostly sequential</td>
</tr>
<tr>
<td>Information Security</td>
<td>Extremely or may be completely secure</td>
<td>Security is a serious issue</td>
</tr>
</tbody>
</table>

6- Conclusions

In this article we presented a new perspective of the quantum computer and how far they are from becoming a reality. And we conclude the followings:

1- Quantum computers are the emerging technology of the 21st century and will be commercially available in the near future.

2- Although the first generation is in its primitive form and expensive, some interested centers have already purchased and installed a quantum computers in their facilities because they believe this technology provide good solution to their complex technological problems.

3- Our perspective about this technology is that it can provide incredible processing speed and storage which greatly outpaces the capacity of available supercomputers; therefore it can provide scientists with amazing opportunities to achieve ambitious progress in science and technology.

4- QC will solve the security issues inherited in the conventional digital computers and there will be no more security concerns when implementing this technology.

5- We encourage young computer scientists and engineers to start looking into this technology, because it is expected to replace...
the conventional computer technology in less than a decade.

7- References


2- Quantum physics by Margaret Rouse, Retrieved on 17/11/2013 from http://whatis.techtarget.com/definition/quantum


4- Chris Davies, Oct 10th 2013, Google using $10m quantum computer to understand Glass future, retrieved on November 2013 from http://www.slashgear.com/google-using-10m-quantum-computer-to-understand-glass-future-10300936/


6- Erica Klarreich, 23-8-2013, Is That Quantum Computer for Real? There May Finally Be a Test, Quantum Magazine.


