Quantum Computing Technology (QCT) - A Data Security Threat

[1]Anil Lamba, [*]Pushparaj, [*]Satinderjeet Singh , Balvinder Singh, and Sivakumar Sai Rela Muni
[1]Department of Computer Science, Charisma University, Turks and Caicos Islands
[2]Lecturer, ECE Dept. ICL Group of Colleges, Ambala, Haryana, India.

ABSTRACT

Advancements in computer science and technology make quantum computation increasingly possible, which would result in unprecedented computational efficiency and allow quantum physicists and chemists to completely model complex quantum mechanical systems. Quantum algorithms have already shown significant advantages over classical algorithms in terms of both runtime and power. Quantum computation opens up new research opportunities in areas such as machine learning, mathematics, and cryptography. However, quantum computation could also pose a danger to online data security.

Keywords: Quantum secure direct communication (QSDC); Quantum Cryptography; Quantum Key Distribution ; Password-based Key Exchange; Everlasting Security; security of data; telecommunication security; Encryption; reliable security alternative

1. Introduction

Alan Turing catalyzed the beginnings of computer science when he conceived the idea of a programmable machine; this was, of course, the Turing machine, revealed to the world in 1936. Since then, generations of scientists worked to bring today's society the modern computer. With these innovations came immense progress in efficient calculations and communication.

While computers today perform algorithmic tasks more quickly than Turing could have ever imagined, researchers in computer science are proposing an even faster method of computation on the basis of quantum mechanical theory. These quantum computers have the potential to significantly outperform their classical counterparts and provide un-precedented computational power. This paper investigates the inner workings and potential applications of quantum computers, proposes viable materials for constructing a quantum computer, discusses monetary restrictions on quantum computer construction, and assesses the impact of quantum computation on data security.

2 Background

Nobel laureate Richard Feynman first raised the idea of quantum computation in 1982 when he commented on the difficulty of simulating quantum processes. Because of the vast amount of information needed to solve the Schrodinger equation - and thus completely describe a quantum system - calculations and simulations of more than two atoms can only be approximated. This problem inspired the creation of methods such as density functional theory (DFT), a computational method that approximates quantum mechanical calculations at a high degree of accuracy. Feynman proposed that one could exactly simulate quantum systems on a quantum-based machine. If true, this prediction provides a world of intrigue to physicists and chemists alike. For the first time, chemists will be able to calculate bond distances and energies without the use of any approximations. In order to construct a computer based on quantum mechanics, one must control individual atoms and electrons, thus achieving complete control over a quantum system. In essence, the key to quantum computing lies in using a more easily controlled quantum system to model another quantum system.

Only three years after Feynman's proposition, David Deutsch constructed a mathematical model for a quantum computer that could produce simulations of physical systems beyond the abilities of the classical Turing machine. Not long after, Peter Shor and Lov Grover published their respective factoring and search algorithms, which greatly surpassed the scope of any previous classical algorithms. Although these and other researchers made impressive progress in the theoretical development of quantum computers, lack of viable hardware and other difficulties prevented successful construction of a physical quantum computer until recently. In 2016, International Business Machines (IBM), launched a cloud-based quantum computer open for public. Researchers are able to use the quantum computer as well as quantum computer simulators to run calculations. In making this cutting-edge technology publicly accessible, IBM hopes to encourage the advancement of quantum computation and open the door to researchers and software developers around the world.

Classical vs. Quantum Systems

The fundamental workings of classical and quantum computers initially appear very similar. Both types of machines process information in bits. However, two important properties distinguish a quantum system from a classical one: superposition and entanglement.

Superposition is the ability to form a linear combination of two states. In a classical system, a bit is represented as either a 0 or 1. A bit can only take on one of these two states. A quantum bit (qubit), on the other hand, can form a superposition of the states

and 1. The state of a qubit is represented using Dirac notation: $\alpha|0\rangle + \beta|1\rangle$. $|0\rangle$ represents the matrix $\begin{bmatrix}1\\0\end{bmatrix}$, and $|1\rangle$ represents the matrix $\begin{bmatrix}0\\1\end{bmatrix}$. Once measured, the qubit will take

on the state 0 with a probability of α□ or 1 with a probability of β□. This superposition of states can be represented graphically as vectors on the Bloch sphere (Figure 1). Superposition is integral to the mathematical operations behind quantum computation and effectively allows the computer to perform several calculations simultaneously.

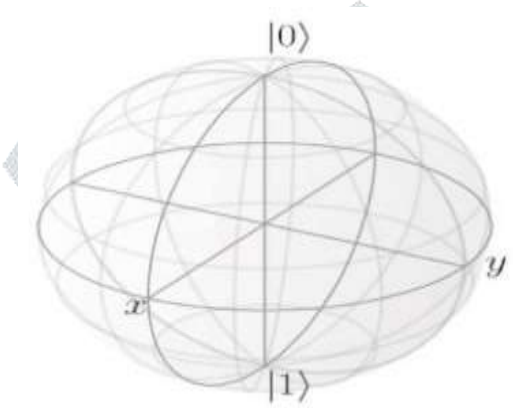

Figure 1. The Block Sphere represents all the possible linear combinations of state for a qubit.

Another key aspect of quantum computing is entanglement, a property in which measuring one qubit yields information about another qubit. Quantum entanglement is particularly useful when measuring a very large set of data. In a classical system, retrieving information about an entire set of data requires a large number of measurements. Quantum entanglement, however, allows a quantum system to retrieve the information using only one measurement.

Qubits and Quantum Circuits:

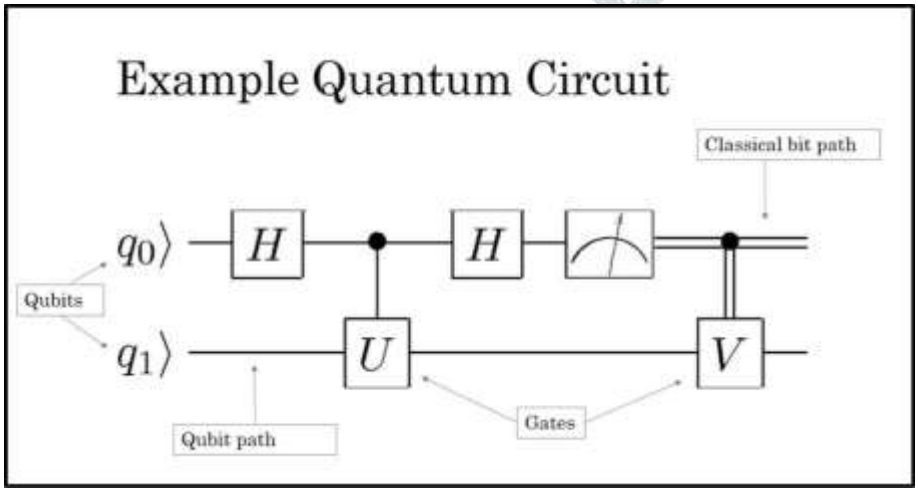

Figure 2. Quantum circuit diagram, modified from Massachusetts Institute of Technology's quantum circuit viewer QASM.

Entanglement, superposition, and several other qubit operations can be illustrated through the quantum circuit diagram (Figure 2). The diagram is read from left to right, and each operation is written in the order it occurs. The horizontal lines each represent a separate qubit. Boxes—called gates—represent specific operations that change the value of each qubit. Mathematically, the gates are represented as matrices, and the results of each gate are obtained through matrix multiplication. Other important operations are the Z-Gate and the Hadamard Gate. Table 1 gives a list of gates and their results. Several operations combine to form quantum algorithms.

Table 1. Common quantum gates and corresponding matrix forms

Example Gate:

One example of a common qubit operation is the NOT Gate. It is represented mathematically as the 2×2 matrix $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$. A single qubit system is represented by the matrix $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$.

To obtain the result of a NOT Gate, multiply the two matrices.

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

The result is the matrix $\begin{bmatrix}\beta\\ \alpha\end{bmatrix}$. Thus, a NOT Gate switches the coefficients of 0 and 1. This process can be written in Dirac notation as:

$$\alpha|0\rangle + \beta|1\rangle \qquad \alpha|1\rangle + \beta|0\rangle$$

Gate	Matrix	Explanation
NOT (also X)	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	switches α and β, rotates the state about x-axis of Bloch sphere
CNOT	$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$	changes the state of the second qubit if the first qubit is in state |1⟩
Y	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$	rotates the state about the *y*-axis of Bloch sphere
Z	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$	rotates the state about the *z*-axis of Bloch sphere
Hadamard	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	puts the qubit in a state exactly between |0⟩ and |1⟩ (superposition)

Quantum Algorithms

Any general computation involves an input, an algorithm that changes the input, and an output. While classical algorithms must often methodically examine each input value separately, quantum algorithms exploit superposition and entanglement in order to examine several values simultaneously. Because of the probabilistic nature of qubits (due to superposition), quantum computers run probabilistic algorithms with bounded error. These algorithms return a result that has a high probability of being correct. Because a probabilistic algorithm does not need to return a result with 100% certainty, it does not need to measure exactly every element of the input, thus significantly decreasing computation time. This improved efficiency is known as *quantum speedup*—the potential for quantum algorithms to outperform classical ones by reducing the number of steps for a given process. Quantum speedup one of the most popular reasons for furthering quantum algorithm development.

Computer scientists evaluate algorithm efficiency by comparing the size of the input n to the number of calculations the algorithm requires. An algorithm is considered efficient if it runs in polynomial time, meaning the algorithm requires *nx* calculations where *x* is a constant. On the other hand, less efficient algorithms run in exponential time, in which the algorithm requires *xn* calculations in order to reach the output. The two most notable algorithms that demonstrate quantum speedup are Shor's algorithm for factoring large integers and Grover's algorithm for searching randomized data sets.

Shor's quantum factoring algorithm, published in 1995, factors large numbers in polynomial time, a feat that classical algorithms can only accomplish in exponential time. The problem of factoring large integers has long been of interest to number theorists. While factoring may seem simple for relatively small integers (three digits or less), the problem becomes increasingly more complex as the input sizes grows. In fact, the task is so difficult that it forms the basis of several cryptosystems. Shor's algorithm tackles the challenge of factoring through the use of the Quantum Fourier Transform, a function analogous to the classical Fourier transform. Many computer scientists point to Shor's algorithm as a prime example of quantum speedup and the sheer mathematical power behind quantum computation. However, the application of this algorithm could mean the end to modern cryptography and data security.

Grover's search algorithm tackles another sought-after mathematical feat: finding a specific value in a set of unordered numbers. The most common application of this algorithm would be to find the minimum value of a list of numbers. While searching an unordered list may seem a trivial task, it proves quite difficult to classical computers. The only classical method of finding a specific value in a list would be to examine each number in the list until the desired value is found. Given a set of numbers of size *n*, a classical algorithm would need on average $0.5n$ steps to find the minimum (Grover, 1997). Grover's quantum algorithm, however, is capable of finding the value in only $0\sqrt{n}\rangle$ steps.

Shor's and Grover's algorithms provide excellent examples of the power behind quantum computation. The widespread use of quantum algorithms could uncover a world of unsolved mathematics problems and innovative methods for completing certain tasks. However, quantum algorithms are difficult to construct because most computer scientists and developers are rooted in classical - as opposed to quantum - physics. IBM addresses this issue in part through the opening of its cloud-based quantum computer simulator. Public access to quantum computing software shall encourage further development of quantum algorithms.

Construction

Quantum computation serves as a classical example of theoretical research preceding experimental research. While researchers began studying quantum computation in the 1980s, major industries have only produced small quantum computers within the last several years. Many materials have been proposed for qubits, common examples being electrons in the excited or ground state, polarized photons, and particles with nuclear spin. One material that is particularly promising, however, is the single-molecule magnet (SMM). The single-molecule magnet exhibits both classical and quantum properties and takes on two separate magnetic spin states, making it a viable candidate for use as a qubit.

Originally proposed as a new material for memory storage, the single-molecule magnet also has potential in quantum computing. A single-molecule magnet exists in two different magnetic spin states and—with enough energy—can switch between these two states. However, SMMs can pass through this energy barrier via the quantum tunneling effect. By exploiting quantum tunneling to switch the SMM's spin states, one can produce the superposition of states required for quantum computing. In addition, interactions known as magnetic exchange coupling allow for entanglement between several SMMs.

Although there are several options for materials to construct quantum computers, another challenge lies in keeping the computers running. One important facet of quantum computation is the prevention of *decoherence*, in which quantum materials lose functional ability through interaction with the environment. To prevent de-coherence, qubits must be kept as isolated as possible. This proves difficult, however, since the qubits must interact with the environment in order to be measured. One solution to preventing outside influence is super cooling. For example, the D-Wave quantum computer in Canada is kept at -273 C°, a mere 0.15° above absolute zero. Although extreme, methods such as this keep qubits functioning as long as possible, allowing researchers to fully explore the applications of quantum computing.
If institutions want to construct and maintain quantum computers, they must also find a source of funding. While government grants and generous donors may contribute to quantum computer construction funding, the gaming industry could be the quantum computer's strongest ally. Several technologies used in scientific research today, such as the graphics processing unit (GPU) and virtual reality software, were originally released for video gaming. Recreational applications are more easily understood (and often more appreciated) by the public, and thus very commercially successful. Appealing to both the scientific and gaming markets could kickstart the widespread construction of quantum computers.

Applications of Quantum Computation: Quantum Machine Learning

The speedup and power behind quantum computation unlock a world of interdisciplinary applications, especially in machine learning. The primary goal of machine learning is to program a computer to recognize and categorize data patterns. The promising aspect of quantum machine learning lies in the quantum computer's ability to simulate quantum systems, a task classical computer cannot do. If quantum computers can produce data that classical computers cannot produce, perhaps they can also interpret patterns that classical computers cannot interpret. This property would benefit several current machine learning projects, from teaching computers to recognize handwritten numbers to

making a program that uses MRI scans to identify mental health risks. The ability to analyze complex data patterns would even help advance research in quantum mechanics. Quantum machine learning could be used to study quantum data more effectively, thus gathering even more information on quantum mechanics itself. Another advantage to quantum machine learning is that general machine learning algorithms are inundated with matrix operations, calculations that form the basis of quantum mechanics. As a result, quantum computers would run machine learning algorithms exponentially faster than classical computers. Several researchers have already written quantum machine learning algorithms and anticipate future use of quantum machine learning.

Consequences of Quantum Computation

While quantum computers have the potential to provide significant advances in technology, widespread quantum computation poses several threats to cybersecurity and cryptography. Because modern cryptography plays a role in nearly every online interaction, it easily goes unnoticed. However, cryptography ensures the security of personal, corporate, and government data. Passwords, credit card information, social security numbers, and private communications all fall under the umbrella of cyber secure data. Cryptographic methods keep this private information safe from third-party intruders largely by exploiting the classical computer's inability to factor large numbers easily. Unfortunately, Shor's factoring algorithm demonstrates the quantum computer's ability to break these methods. Should quantum computers become readily available, all protected data will suddenly be at risk. Incidentally, this threat has resulted in an entirely new field of research: quantum cryptography.

A New Field is Born: Quantum Cryptography

Cryptography dates back as far as the time of Caesar. One of the most popular ciphers is indeed the Caesarean cipher, in which one assigns a number value to each letter of the alphabet (i.e. "a" is 1, "b" is 2, "c" is 3, etc.) and sends a message entirely composed of these numbers. The recipient of the code can then decode it based on his or her knowledge of the assigned letter values. This type of encoding and decoding is known as *private key cryptography*, in which two parties decide on a key that encodes and decodes the secret messages. This method will only prevent interception bya third party if the two parties can keep the key completely private. This is a difficult task, since the two parties must somehow communicate the key without being intercepted.

The other main branch of cryptography is *public key cryptography*. In public key cryptography, each party publishes a key to encode a message, but withholds the key to decode the message. For instance, if Person A wishes to send a secret message to Person B, Person A will simply look up Person B's public encoding key, encode the secret message, and send the message to Person B. Person B then decodes the message using his or her secret decryption key. Making the encoding key public seems counter-intuitive, especially since many decoding keys can be inferred by reversing the encoding key. Public key cryptography is a very secure method of communication, however, if one takes advantage of one-way mathematical operations. These operations are simple to do forward but very difficult to do in reverse. For example, squaring a number is a lot easier than taking the square root of a number. More complicated one-way mathematical operations form the basis of public key cryptography.

One of these one-way mathematical operations involves factoring large integers. While it is elementary to multiply several prime numbers, it is much more complex to do this process in reverse by finding the factors of a very large number. The most popular encryption technique based on factorization is the Rivest-Shamir-Adleman(RSA) technique. Until recently, this method has been very secure due to the classical computer's inability to factor large numbers efficiently. In light of quantum computation and Shor's factoring algorithm, cryptographers are frantically searching for an encryption system that can withstand attacks from quantum computers. The solution lies in writing quantum algorithms for encryption, thus creating quantum cryptography.

Besides generally protecting information from quantum hackers, the use of quantum computers in cryptography provides myriad advantages. Compared to classical computers, networking quantum computers require exponentially less communication to solve problems. Efficient computer communication is vital for a secure cryptosystem. Quantum laws such as the no-cloning theorem and uncertainty principle also provide extra security against third-party attackers.

Conclusions

Quantum computers provide innumerable advances in technology. Algorithms such as Shor's and Grover's demonstrate that quantum computers can perform certain operations much faster than classical computers and reach impressive mathematical milestones. In addition, the use of quantum computers would allow quantum physicists and chemists to study and simulate quantum systems much more accurately than any classical method. Machine learning would likewise benefit from quantum computation through the quantum computer's ability to produce (and potentially interpret) complex data patterns and more efficiently implement machine learning algorithms.

Quantum algorithms are appealing because they allow access to novel solutions to complicated problems. Shor's and Grover's algorithms gained publicity because they could perform tasks that classical algorithms could not. There are

several other quantum algorithms that do not receive as much attention because they accomplish tasks classical computers can already accomplish in a timely manner. The most significant gain from quantum computers will be in algorithms that solve problems which classical algorithms cannot.

Before the world completely switches to quantum computation, however, much progress must be made. Quantum algorithms require a completely different way of thinking about problem-solving. Even if one does build a large-scale quantum computer, software developers must have enough knowledge of quantum theory to write code for the machines. Addressing this issue, IBM's quantum computer and quantum computer simulator encourage experimentation with quantum computer coding.

Other obstacles to quantum computing include the high cost of materials and budget funding. Although quantum computation has widespread applications in many fields such as chemistry, physics and mathematics, marketing quantum computation to the video gaming industry might propel its development the most. Quantum computer developers must adapt and respond to challenges such as these if they are ever to produce large-scale quantum computers.

REFERENCES

[1] Sharmaa, V., & Balab, M. (2019). A Scheduling Strategy for Cloud Computing with Improved Processing Time. International Journal of Grid and Distributed Computing, 12(2), 54-62.

[2] Walia, A., & Pal, P. (2014). An implemented approach of VANET using location information based technique for safe city and vehicle. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2, 400-405.

[3] Grover, L., Verma, L. P., & Mathuria, A. (2012). Comparison between SAR and NSAR in MANETs. International Journal of Data & Network Security, 1(1).

[4] Aggarwal, P., & Pal, P. (2014). A Review of complexity method for wireless Channel Estimation using a BEM. 2(Xii), 590–593. Retrieved from www.ijraset.com

[5] Chauhan, J., & Pal, P. (2014). International Journal of Research and Science Engineering Technology (I J R A S E T) A Review to Vho for Wimax and Wifi Networks. 2(Ix), 114–117.

[6] Grewal, K., Scholor, M. T., & Pal, P. (2001). Innovative Research in Applied Science and Technology A Study of Wireless Power Transmission:Good Bye wires. 50–55.

[7 Kadian, A. K., Pal, P., & Goyal, V. (2013). Concept of Dynamic Bandwidth Allocation and Scheduling Algorithms in Passive Optical Networks. International EJournal of Mathematics and Engineering, 224, 2195–2200. Retrieved from www.internationaleJournals.com

[8] Kapoor, S., Pal, P., Gupta, S., & Sharma, M. (2014). Stable AODV Protocol in Mobile Ad-Hoc Network. International Journal of Advanced Research in Computer Science and Software Engineering, 4(6), 2277. Retrieved from www.ijarcsse.com

[9] Kaur, A., Pal, P. K., & Pal, P. (2014). An Efficient Way of Broadcasting Response Message to Help Demanding Vehicle in VANET. 2(Xii), 546–548.

[10] Vinod Kumar, Anil Kumar, Pushpraj Pal, (2012), 'Image Denoising Using Hybrid Filter' 1(1), 10–12. Retrieved from www.cirworld.com

[11] Mathuriya, A., Pal, P., & Grover, L. (2003). Stability Aware Routing in Mobile Ad-Hoc Networks using multiple Route. International Journal of Computers & Technology, 2(3c), 163–170. https://doi.org/10.24297/ijct.v2i3c.2716

[12] Singh, A., Pal, P., Gupta, S., & Singh, H. (2014). A Novel Proposed Approach to find an Optimal Path in DSR. 2(X), 405–408. Retrieved from www.ijraset.com

[13] Verma, A., & Pal, P. (2014). Simulation to maximize retransmission of packets in WMSN. 2(Xii), 582–589. Retrieved from www.ijraset.com