8th International Conference on
Combinatorics, Cryptography, Computer Science and Computation
November. 15-16, 2023

The prospect of cryptography and computing with quantum computers

Mahdi Imanparast[1]
Department of Computer Science, University of Bojnord, Bojnord, Iran

Abstract

Despite the significant improvements in the efficiency and speed of computing processors, there are still complicated problems that even existing supercomputers cannot solve. They mean solvable problems that often have high computational complexity (usually of exponential order) that require days or years to solve. Quantum computers, which are defined based on the concepts of quantum physics, opened a new window for researchers in the field of computer science and computing. Although, the introduction of quantum algorithms such as Shor's algorithm promised a faster solution to some problems in the computer world that would take years to solve with classical computers, in reality, quantum computers face serious challenges in terms of hardware and implementation. In this paper, while reviewing the basics of quantum computers and their achievements, we discuss their challenges and prospects in the field of cryptography and computing.

Keywords: Computational models, Quantum computers, Quantum physics, Qubits.
AMS Mathematical Subject Classification [2010]: 03D15, 68Q12

1 Introduction

When scientists and engineers are faced with difficult problems, they turn to supercomputers, which often have very large numbers of processor cores. With the increase in the memory and speed of computers, some complicated problems have been solved and their number has been reduced, but there are still some problems that cannot be solved even by supercomputers and require years of time to solve them. In addition to the existence of a complicated problem, a more basic issue in the process of developing and manufacturing chips is reducing the dimensions of transistors. As the dimensions of transistors reduce, in structures below 10 nm, their dimensions close the atomic dimensions. These tiny transistors no longer work according to the laws of classical physics like the old transistors and follow the more complex laws of quantum physics. A traditional computer might do things like sort through a large database of molecules, but it would unable to solve more complicated problems, like simulating how those molecules behave, because no computer has the memory and ability to handle all possible permutations of molecular behaviour. Quantum computers take a new approach to these kinds of complicated problems by creating multi-state computing spaces.

Quantum physics describes the laws that govern the microscopic world of atoms and subatomic particles. Quantum computing brings together ideas from information theory, computer science, and quantum physics.

[1]speaker

The topic of quantum computing started with two physicists and researchers of IBM named Rolf Landauer and Charles Bennett. In 1960, Landauer proposed that information has a physical nature that can change according to physical laws. In 1981, Paul Benioff of Argonne National Laboratory attempted to build a machine that looked like a regular computer but operated according to the laws of quantum physics. In 1982, famous physicist Richard Feynman demonstrated how a basic machine could be used to perform calculations using the principles of quantum mechanics. He argued that a quantum computer is capable of simulating physical phenomena that a traditional computer cannot. A few years later, David Deutsch, one of the most influential people in the development of quantum computing, described the theoretical foundations of a quantum computer [1].

Quantum computers take advantage of the unique behaviours of quantum physics, such as superposition and entanglement, and apply them to computing. Conventional computers work on binary bits, but quantum computers transfer information through quantum bits, or qubits. Qubits behave very differently from bits because they are made of quantum particles found in nature. While bits always represent 0 or 1, a qubit, in addition to 0 or 1, can be a superposition of 0 and 1 at the same time. The best way to imagine superposition is to imagine a coin toss. For a throwing coin, at any moment two states can be considered, tail and head. The qubits can be physically connected to each other to generate another quantum property called entanglement, which means that with each qubit added to a system, the machine's capabilities, the amount of information, and its processing ability increase exponentially.

From the numerical aspect, a qubit can be considered a two-dimensional vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the Hilbert vector space, which is a linear combination (or superposition) of two basic states $|0\rangle$ and $|1\rangle$, where α and β are complex numbers ($\alpha, \beta \in \mathbb{C}$) and satisfy the condition $|\alpha|^2 + |\beta|^2 = 1$. During measurement, the state of a qubit collapses to one of the bases of $|0\rangle$ and $|1\rangle$. In fact, the qubit $|\psi\rangle$ will be in state $|0\rangle$ with probability $|\alpha|^2$ and in state $|1\rangle$ with probability $|\beta|^2$. A comparison between the structure of classical bits and qubits is shown in Figure 1.

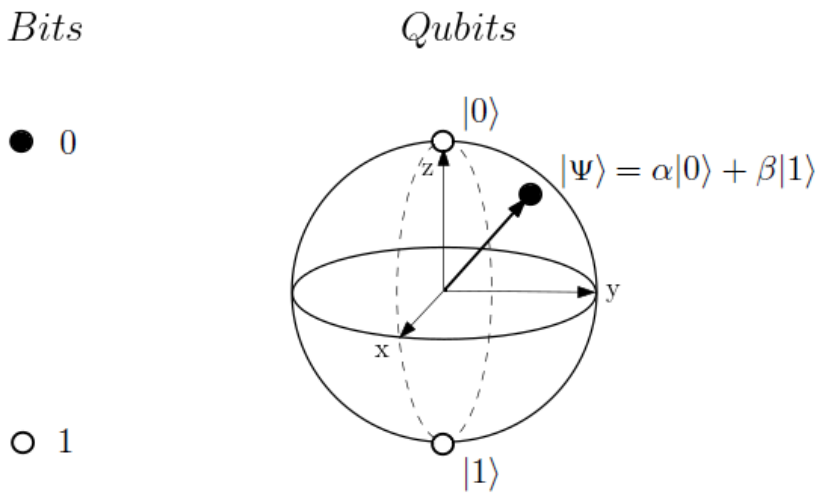

Figure 1: The structure of bits compared to qubits.

In order to create qubits, which are the main building blocks of quantum computers, scientists must find the smallest particles in nature and create them by manipulating atoms or special methods of nano-engineering artificial atoms. One of the most advanced approaches in making qubits is the use of super-

conducting qubits, which are made of electrons and are known as luster-like quantum computers. Another approach that is on the rise is trapped ions, and another method is based on quantum particles of light called photons.

2 Achievements of quantum algorithms

Quantum computers can simultaneously store all the different states of a problem or its solutions in their qubits. Therefore, they need much less memory, because in a conventional computer, such processes require a separate space to be allocated to each solution. Therefore, when qubits are processing, quantum computers can process information simultaneously, which brings a great speed in performing calculations compared to a conventional computer. Quantum computers are expected to be great at solving a certain class of problems, but this does not mean they will be better tools than traditional computers for every application. It should be noted that problems that are basically unsolvable by so-called traditional algorithms are also unsolvable by quantum algorithms.

One of the early advances and one of the strongest arguments in the field of quantum computing to date is Shor's quantum algorithm for computing the prime factors of integers, which is considered a complicated problem for traditional computers. This algorithm which is presented by Peter Shor [2] in 1994, can compute the prime factors of a large integer in polynomial time. Note that the calculations of this problem by the most powerful supercomputers available may take months or years. This algorithm has important implications in cryptography, as many encryption methods rely on the difficulty of computing prime factors of large integers. Another example is Grover's quantum search algorithm, which was proposed by Lov Grover [3] in 1996. This quantum algorithm can search for an element in a large unstructured or unordered database with N input in $O(\sqrt{N})$ time, while a conventional algorithm takes $O(N)$ time.

One of the major developments in quantum computing came in 2017, when IBM researchers model beryllium hydride, the largest molecule simulated on a quantum computer to date, and in 2019, IonQ researchers do an even bigger impression, simulation of water molecule using quantum computing. A quantum computer cannot do everything faster than a conventional computer, but there are several areas where quantum computers have the potential to make a big impact, including cryptography, optimization, quantum machine learning, searching large databases, and modelling molecular structures. One of the most important applications of quantum computers, which are expected to become superpowers in this field, is when dealing with atoms and molecules, because quantum computers can simulate different models at the same time and make a lot of contributions to medicine and pharmacy science.

3 Hardware status of quantum computers

In the early years, the discussion of qubits and quantum computers was only on paper, but in 2000 two significant developments occurred in this area of physics. Isaac Chuang, a professor at MIT and a researcher at IBM, could build a real quantum computer with 5 qubits using fluorine atoms. In the same year, researchers at Los Alamos National Laboratory built a 7-qubit machine. Five years later, researchers at the University of Innsbruck were able to add one qubit to the same machine and build an 8-qubit machine. Until 2011, many researches have done in this field. But this year, the pioneer Canadian company D-Wave did an effective step in the development of the world of quantum computing by presenting a 128 qubit computer. In

2015, Google developed its quantum computer based on D-Wave's design and announced that it had found a new way to control and detect quantum errors. Table 1 summarizes the quantum computers presented by various institutions that have worked in this area.

In 2017, Microsoft introduced a new programming language called $Q\sharp$ to work on algorithms and create quantum programs. Microsoft, Amazon, Google, IBM, IonQ, D-Wave and some other companies provide quantum tools based on cloud computing space where users can use small-scale quantum processors online. Some of these quantum environments include Microsoft's Azure Quantum, IBM's IBM Quantum Experience, and Amazon's AWS Braket. Between the years of 2000 and today, extensive researches have been done in the field of building and developing the hardware of quantum computers, of which we mentioned only a small part above. Despite these advances, there are still many obstacles that quantum computers face them.

Table 1: Some quantum computers have been built so far.

Year	**Product/ institution name**	**Number of qubits**
2000	Issac chuank in IBM	5
2000	Los Alamos National Laboratory	7
2005	University of Innsbruck	8
2011	D-Wave One	128
2013	D-Wave Two	512
2015	D-Wave 2X	1152
2017	D-Wave 2000Q	2048
2018	Bristlecone Google	72
2019	IBM Q System One	20
2019	Intel	49
2021	IBM's Ospery	433

4 Challenges of quantum computers

In order to qubits have significant calculations, they must number in the thousands or even millions. At the same time, increasing the number of qubits in processors is very challenging, because it is difficult to keep the particles that make up qubits in the quantum state, and any environmental disturbance may cause the loss of the quantum state and their superposition and entanglement properties. This makes it difficult to maintain the delicate quantum state of qubits and perform accurate and reliable computations. To reduce the effectiveness of quantum systems from the outside environment, expensive equipment is usually needed to provide a very high vacuum and a temperature close to absolute zero.

Studies by scientists at several major research centers in 2021, estimated that breaking advanced encryption in 8 hours would require 20 million qubits. On the other hand, the higher number of qubits, increase the probability of device error, because in this case, precise control of a large number of quantum systems is required. This could mean devoting a large portion of the qubits to error-correction routines that keep the calculations on track. Currently, despite the small number of qubits in existing quantum computers, it is not possible to allocate qubits for this purpose. In quantum computing, errors are much more difficult to detect and correct due to the nature of quantum systems [4].

Another fundamental challenge is that many details in a quantum computer must be redesigned. Con-

ventional algorithms cannot be used in quantum computers because the rules are completely different at the most basic levels, and quantum algorithms are difficult to implement in reality. For example, for Shor's algorithm, only prime factors of 15 and 21 have been calculated by existing quantum computers. Therefore, the challenges faced by quantum computing are not only related to hardware. Building and maintaining a quantum computer is very expensive. Because, they need for specialized equipment and trained personnel, which can limit access to quantum computing to certain groups or organizations.

One of the challenges currently facing quantum computers is the problem of not being sure of their answer, because the error correction mechanism in classical computers usually requires extra bits. Furthermore, the instability of qubits means that they are unreliable, and may still cause computational errors. This has given rise to a branch of quantum computing devoted to the development of quantum error correction (QEC) methods.

5 Conclusions

Quantum computing has the potential to make a tremendous progress in the field of computing in highly specialized applications, but it may take several years for this idea to move out of research and laboratory environments, just like the development process of traditional computers. Therefore, it is expected that supercomputers will continue to be used on a large scale, and quantum computers will become more available for specialized research in specific fields. Since the creation of qubits requires special conditions (such as high vacuum or very low temperature), it is unlikely that in the future, a mobile phone or home computer will contain a quantum chip.

The development of quantum hardware is one of the big challenges in this field. Quantum computers must have several thousand qubits to deal with real-world problems, and the quantum computers built so far are far from this goal. On the other hand, creating quantum algorithms that are compatible with the quantum world are not as easy as classical algorithms. Algorithmically, to date, except for a few limited algorithms such as Shor and Grover's algorithms, nothing has been discovered that performs better on quantum computers, and for many problems that can be solved using conventional computers, there are no known quantum algorithms.

Computing and computer science researchers predict that quantum computers will challenge current encryption methods and introduce new possibilities for secure and private communications. If quantum computers manage to perform decryption calculations in a fraction of a second, it will be a great event and at the same time a difficult challenge. Therefore, it is important to work on issues under the title of post-quantum cryptography in order to create a complete and efficient quantum cryptography system in sync with the development of quantum computers.

Quantum computing is our way of mimicking nature to solve incredibly difficult and solvable problems. However, quantum computers are still in their early stages and require further development before they can be widely used. Just as in the 1950s, many of the advances in computers today were unimaginable, in the field of quantum computers, the achievements that researchers predict in this field will take time to be realized. Therefore, quantum computers still have a long way to go.

Without higher numbers of qubits and better error correction, proving the superiority of quantum computing in solving problems is still somewhat far from expected. Building a large-scale quantum computer with a large number of qubits is very difficult because it requires precise control of a large number of quantum

systems and a lot of energy. Currently, the number of qubits that can be controlled and manipulated in a laboratory environment is still very small, limiting the potential of quantum computing. Another fundamental problem of a quantum computer is how to send and receive information from it. Some critics consider this problem insolvable. However, this appears to be less of a problem in optical quantum computers where qubits are defined in terms of photons.

References

[1] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2011.

[2] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM journal on computing, 26 (5), (1997), pp. 1484–1509.

[3] L. K. Grover, *A fast quantum mechanical algorithm for database search*, In Proceedings of the 28th annual ACM symposium on Theory of computing, (1996), pp. 212-219.

[4] M. Brooks; *Quantum computers: what are they good for?*, Nature, 617(7962), (2023), pp. S1-S3.

e-mail: m.imanparast@ub.ac.ir