**QUANTUM COMPUTING**

*Submitted in partial fulfilment of the requirements for the award of the degree of*

**Bachelor of Technology**

**In**

**Computer Science Engineering**

by

**M. RAMACHANDRA KASHYAP**

**PIN No. – 2210316131**

Dept. of CSE

Under the Supervision of

**Ms Kalyani Ghutugade**

Assistant Professor

Dept.of CSE



**Department of Computer Science Engineering**

**GITAM School of Technology**

**GITAM Deemed University**

**Hyderabad Campus**

2018-19

**GITAM School of Technology**

**Deemed to be University**

**(Estd.u/s 3 of the UGC Act, 1956)**

**Hyderabad Campus**

**Accredited by NAAC with ‘A+’ Grade**

**Rudraram Village, Patancheru Mandal, Sangareddy Dist**

**Department of Computer Science Engineering**

**-----------------------------------------------------------------------------**

**CERTIFICATE**

This is to certify that the Technical Seminar work entitled **"QUANTUM COMPUTING"** being submitted by ‘**M. Ramachandra Kashyap' (PIN No:2210316131)** for partial fulfilment of the requirement for the award of **Bachelor of Technology** in **Computer Science Engineering** to GITAM School of Technology, GITAM Deemed University, Hyderabad campus during the academic year 2018 - 2019 is a record of bon afede piece of work, undertaken by him/her the supervision of the undersigned**.**

**ABSTRACT**

A brief introduction to Quantum computers which are a leap forward in modern computing technologies.

Today's computers work on bits that exist as either 0 or 1. Quantum computers aren't limited to two states; they encode information as quantum bits, or qubits, which can exist in superposition. Qubits represent atoms, ions, photons or electrons and their respective control devices that are working together to act as computer memory and a processor. Because a quantum computer can contain these multiple states simultaneously, it has the potential to be millions of times more powerful than today's most powerful supercomputers.

Due to technical obstacles, till date, a quantum computer has not yet been realized. But the concepts and ideas of quantum computing has been demonstrated using various methods like NMR, Ion Trap, Quantum Dot, Optical Methods, etc. A quantum computer manipulates qubits by executing a series of quantum gates, each a unitary transformation acting on a single qubit or pair of qubits.  In applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits in some initial state.  The qubits can then be measured, with this measurement serving as the final computational result.

Research must devise a way to maintain decoherence and other potential sources of error at an acceptable level. Probably the most important idea in this field is the application of error correction in phase coherence as a means to extract information and reduce error in a quantum system without actually measuring that system. Thereby, quantum computers will emerge as the superior computational devices and perhaps one day make today's modern computer obsolete.

CMOS operating at cryogenic temperatures down to 4 Kelvin (cryo-CMOS) allows for closer system integration, thus promising a scalable solution to enable future quantum computers.

**TABLE OF CONTENTS**

**INTRODUCTION1**

**BACKGROUND2**

HISTORY OF QUANTUM COMPUTERS2

QUANTUM COMPUTING BASICS2

**THEORY OF UNIVERSAL COMPUTATION3**

THE UNIVERSAL QUANTUM COMPUTATION3

**ESSENTIALS OF QUANTUM COMPUTER4**

QUANTUM DOTS4

SUPER POSTION AND ENTANGLEMENT5

**CRYO-CMOS6**

WHY DEVICES NEED TO BE BELOW 4 KELVIN6

HOW TO ACHIEVE TEMPERATURES NEAR ABSOLUTE ZERO7

CRYO-CMOS CHARACTERISTICS8

**ADVANTAGES AND DISADVANTAGES OF QUANTUM COMPUTER11**

**APPLICATIONS12**

ARTIFICIAL INTELIGENCE12

MOLECULAR MODELING12

CRYPTOGRAPHY13

FINANCIAL MODELING13

WEATHER FORECASTING14

PARTICLE PHYSICS14

**COMMERCIAL QUANTUM COMPUTER 15**

**CONCLUSION16**

**REFERENCES17**

**LIST OF FIGURES**

[Figure 1 A Quantum Computer Processor at D-wave at about 15 millikelvin 7](#_heading=h.30j0zll)

[Figure 2 Output Characteristics in 160nm CMOS Technology 8](#_heading=h.1fob9te)

[Figure 3 Output Characteristics in 40nm CMOS Technology 9](#_heading=h.1fob9te)

[Figure 4 ID-VG Characteristics in 160nm CMOS Technology 9](#_heading=h.1fob9te)

1. **INTRODUCTION**

Quantum computing is a new paradigm that exploits basic principles of quantum mechanics, such as entanglement and superposition, potentially enabling unprecedented speedups in solving intractable problems. The new computing opportunities include prime factorization, quantum simulations for synthesis of drugs and materials, and complex optimizations. In its fundamental embodiment. The quantum processor consists of a set of quantum bits (qubits) operating at extremely low temperatures, typically a few tens of mK, while the classical electronic controller issued to read out and control the quantum processor, Although the classical controller is implemented today with room-temperature laboratory instruments, this approach becomes increasingly challenging and less cost-effective as the number of qubits grows toward the thousands and millions, as required by practical quantum algorithms .Although other specialized electronic technologies can handle cryogenic temperatures, only CMOS can work down to at least 30 mK while providing complex system-on-chip integration capable of handling thousands or millions of qubits. A drastic reduction of the complex interconnections between the cryogenic chamber and the room-temperature electronics will result in enhanced compactness and reliability, thus paving the way to the creation of practical quantum computers. More-over, the cryo-CMOS circuits and systems could prove useful in other domains, for example, in applications that require cryogenic environments as an integral part of their operation, such as space and high-energy-physics experiments, or wherever extremely low noise is essential, such as in metrology, imaging, and instrumentation. Cryogenic CMOS circuits have been proposed before for applications ranging from space missions to low-noise amplifiers. However, quantum processors require extremely high performance from the classical electronic controller in terms of bandwidth and noise, so as to ensure accuracy and speed in the control and readout of the qubits.

1. **BACKGROUND**

**2.1 History of Quantum Computers**

In 1982, the Nobel prize-winning physicist Richard Feynman thought up the idea of a 'quantum computer', a computer that uses the effects of quantum mechanics to its advantage. For some time, the notion of a quantum computer was primarily of theoretical interest only, but recent developments have bought the idea to everybody's attention. One such development was the invention of an algorithm to factor large numbers on a quantum computer, by Peter Shor (Bell Laboratories). By using this algorithm, a quantum computer would be able to crack codes much more quickly than any ordinary (or classical) computer could. In fact a quantum computer capable of performing Shor's algorithm would be able to break current cryptography techniques in a matter of seconds. With the motivation provided by this algorithm, the topic of quantum computing has gathered momentum and researchers around the world are racing to be the first to create a practical quantum computer.

**2.2 Quantum Computing Basics**

In the classical model of a computer, the most fundamental building block, the bit, can only exist in one of two distinct states, a 0 or a 1. In a quantum computer the rules are changed. Not only can a 'quantum bit', usually referred to as a 'qubit', exist in the classical 0 and 1 states, it can also be in a coherent superposition of both. When a qubit is in this state it can be thought of as existing in two universes, as a 0 in one universe and as a 1 in the other. An operation on such a qubit effectively acts on both values at the same time. The significant point being that by performing the single operation on the qubit, we have performed the operation on two different values.

Likewise, a two-qubit system would perform the operation on 4 values, and a three-qubit system on eight. Increasing the number of qubits therefore exponentially increases the 'quantum parallelism' we can obtain with the system. With the correct type of algorithm it is possible to use this parallelism to solve certain problems in a fraction of the time taken by a classical computer.

**3.Theory of Universal Computation**

One thing that all computers have in common, from Charles Babbage's analytical engine (1936) to Pentium based PC's, is the theory of classical computation as described by the work of Alan Turing. In essence, Turing's work describes the idea of the universal Turing machine, a very simple model of a computer that can be programmed to perform any operation that "would naturally be considered to be computable". All computers are essentially implementations of a universal Turing machine. They are all functionally equivalent and although some may be quicker, larger or more expensive than others, they can all perform the same set of computational tasks.

**3.1 The Universal Quantum Computer**

The Church-Turing principle - "There exists or can be built a universal computer that can be programmed to perform any computational task that can be performed by any physical object".

A number of key advances have been made in the theory of quantum computation, the first being the discovery that a simple class of 'universal simulator' can mimic the behaviour of any finite physical object, by Richard Feynman in 1982. David Albert made the second discovery in 1984 when he described a 'self-measuring quantum automaton' that could perform tasks that no classical computer can simulate. By instructing the automaton to measure itself, it can obtain 'subjective' information that is absolutely inaccessible by measurement from the outside. The final and perhaps most important discovery was made by David Deutsch in 1989, he proved that all the computational capabilities of any finite machine obeying the laws of quantum computation are contained in a single machine, a 'universal quantum computer'. Such a computer could be built from the quantum equivalent of the Toffoli gate and by adding a few extra operations that can bring about linear superpositions of 0 and 1 states, the universal quantum computer is complete. This discovery requires a slight alteration to the Church-Turing principle - "There exists or can be built a universal quantum computer that can be programmed to perform any computational task that can be performed by any physical object".

1. **ESSENTIALS OF A QUANTUM COMPUTER**

A quantum computer is nothing like a classical computer in design; you can't for instance build one from transistors and diodes. In order to build one, a new type of technology is needed, a technology that enables 'qubits' to exist as coherent superpositions of 0 and 1 states. The best method of achieving this goal is still unknown, but many methods are being experimented with and are proving to have varying degrees of success.

**4.1 Quantum Dots**

An example of an implementation of the qubit is the 'quantum dot' which is basically a single electron trapped inside a cage of atoms. When the dot is exposed to a pulse of laser light of precisely the right wavelength and duration, the electron is raised to an excited state: a second burst of laser light causes the electron to fall back to its ground state. The ground and excited states of the electron can be thought of as the 0 and 1 states of the qubit and the application of the laser light can be regarded as a controlled NOT function as it knocks the qubit from 0 to 1 or from ' to 0.

If the pulse of laser light is only half the duration of that required for the NOT function, the electron is placed in a superposition of both ground and excited states simultaneously, this being the equivalent of the coherent state of the qubit. More complex logic functions can be modelled using quantum dots arranged in pairs. It would therefore seem that quantum dots are a suitable candidate for building a quantum computer. Unfortunately, there are a number of practical problems that are preventing this from happening:

The electron only remains in its excited state for about a microsecond before it falls to the ground state. Bearing in mind that the required duration of each laser pulse is around 1 nanosecond, there is a limit to the number of computational steps that can be made before information is lost.

Constructing quantum dots is a very difficult process because they are so small. A typical quantum dot measures just 10 atoms (1 nanometre) across. The technology needed to build a computer from these dots doesn't yet exist.

To avoid cramming thousands of lasers into a tiny space, quantum dots could be manufactured so that they respond to different frequencies of light. A laser that could reliably retune itself would thus selectively target different groups of quantum dots with different frequencies of light. This again, is another technology that doesn't yet exist.

**4.2 Super Position and Entanglement**

It’s only when you look at the tiniest quantum particles — atoms, electrons, photons, and the like — that you see intriguing phenomena like superposition and entanglement.

Superposition refers to the quantum phenomenon where a quantum system can exist in multiple states or places at the exact same time. In other words, something can be “here” and “there,” or “up” and “down” at the same time.

Entanglement is an extremely strong correlation that exists between two or more quantum particles. So strong, in fact, that the quantum particles are inextricably linked in perfect unison, even if separated by great distances. The particles are so intrinsically connected, they “dance” in instantaneous, perfect unison, even when placed at opposite ends of the universe. This might seem well impossible, but is fundamental to quantum world. Einstein, intrigued by the mind-bending phenomenon, described entanglement as “spooky action at a distance.”

A composite system can be expressed as a sum or superposition of products of the individual states of the local constituents.

Superposition helps do away from binary constraints. The working of a quantum computer is based on using the particles in superposition. Rather than representing bits, such particles represent qubits, which can take on the value 0, 1, or both simultaneously.

Quantum computer can hold the information using a system that can exist in two states at the same time. This is possible due to the superposition principle of quantum mechanics. This “qubit” can simultaneously store a “0” and “1.” Similarly, two qubits can simultaneously hold four values: 00, 01, 10, and 11.

**5. Cryo-CMOS**

**5.1 Why devices need to be below 4 kelvin temperature**

quantum computers are typically created from 2 basis states, usually thought of as “0” and “1”. Now, pretend for a moment that these were the only two possible states (aka we were using a classic computer architecture). It’s not too hard to imagine that it takes some energy to change from 0 to 1 or from 1 to 0. Right? In fact, usually 0 and 1 are implemented by defining ranges of electrical voltages, where one range is classified as 0, and the other as 1. So for example, 0–2 volts could be considered a “0”, while as 5–7 could be considered a “1”. In that case, we literally need energy to move from one state to another.

Ok, cool. So let’s go back to a case where we can have quantum states in addition to our two basis states. Going back to our voltage range example, we now need to figure out how we can define ranges somewhere in there for the quantum states.

Most computers use ranges with extremely small gaps in between the ranges to represent the quantum states. So for example, if we had three contiguous quantum states (which we will call A, B, and C), their voltage ranges might be 0.5–0.75 V for quantum state A, 0.751–1.01 for quantum state B, and 1.02–1.27 for quantum state C respectively. That’s not a lot of room for error to begin with, and the gaps between these ranges are usually much smaller.

So think about it, if you get a tiny amount of error in your voltages, you could easily accidentally push a qubit from quantum state A to quantum state B. Or from B to C. Or from B to A.

This leads to the idea of why we need our quantum computers to be so cold. At extremely cold temperatures, atoms and molecules simply move around less. The lower a temperature is, generally speaking, the more stable a molecule becomes. Less movement means less energy being expelled.

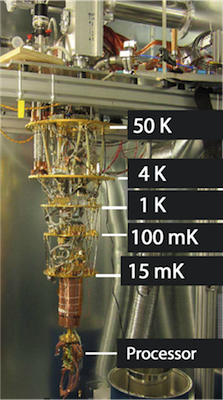
At a molecular level, that means that less energy is flying around, and consequently (since voltage and energy are directly related) less volatility in the voltage. That means that there’s less of a chance that something outside of a human’s control will cause a qubit’s voltage to spike, causing the qubit to flip from one quantum state to another.

And that’s it. By keeping the computer cold, we are introducing less energy into the system, and thus minimizing the chances of qubits incorrectly flipping in between quantum states.

**5.2 How to Achieve Temperature Near-Absolute Zero**

Reduction of the temperature of the computing environment below approximately 80mK is required for the processor to function, and generally performance increases as temperature is lowered - the lower the temperature, the better. The latest generation D-Wave 2000Q system has an operating temperature of about 15 millikelvin. The QPU and parts of the input/output (I/O) system, comprising roughly 10kg of material, is cooled to this temperature, which is approximately 180 times colder than interstellar space! Most of the physical volume of the current system is due to the large size of the refrigeration system. The refrigeration system used to cool the processors is known as a dilution refrigerator.

To reach the near-absolute zero temperatures at which the system operates, the refrigerators use liquid helium as a coolant. The type of refrigerator inside the D-Wave system is known as a "dry" dilution refrigerator. This means that all the liquid helium resides inside a closed cycle system, where it is recycled and decondensed using a pulse-tube technology. This makes them suited to remote deployment, as there is no requirement for liquid helium replenishment on-site

.

#### Figure 1. A Quantum Computer processor at D-Wave lab achieving temperatures about 15 millikelvin

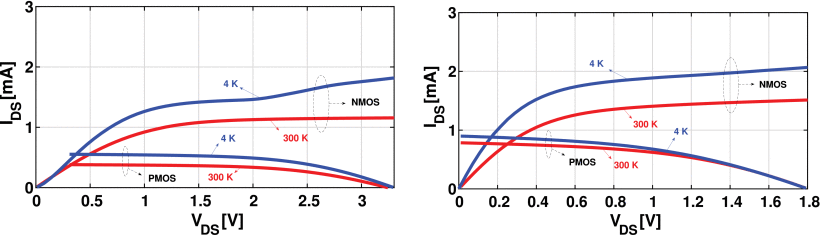
​

The specialized equipment to allow cooling to these temperatures is available commercially and runs reliably. The refrigeration technology is also mature enough that the system has a turnkey operation. The computer can be cooled down to operating temperature within several hours, and once this temperature is reached remain cold for months or years.

**5.3 Cryo-CMOS Characterization**

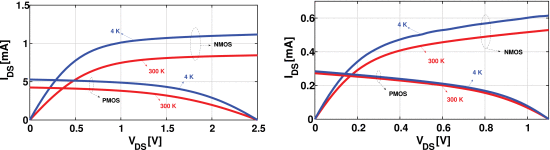
The first challenge to address when designing CMOS circuits at cryogenic temperatures is the availability of device models. Figs. 3 and 4 show the measured *ID* -*V*DS characteristics for both NMOS and PMOS transistors at 300 and 4 K in 160- and 40-nm CMOS technologies, respectively. As expected, the drain current at 4 K is higher than that measured at 300 K, mainly due to increased carrier mobility. The mobility-induced current increase is partially mitigated by the increase in threshold voltage for both thin-oxide 160-nm NMOS and PMOS. In addition to a large variation of the transistor parameters, specific cryogenic non-idealises can be present, such as a kink and hysteresis. For example, the thick-oxide transistors in 160-nm CMOS show a clear kink at higher *V*DS, due to the bulk current generated by impact ionization at the drain combined with increased resistivity of the frozen-out substrate, leading to a decrease in the threshold voltage. As an additional challenge, prior work suggests that mismatch deteriorates at cryogenic temperature.

[Figure 3](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/4/8241022/8036394/patra3ab-2737549-large.gif)



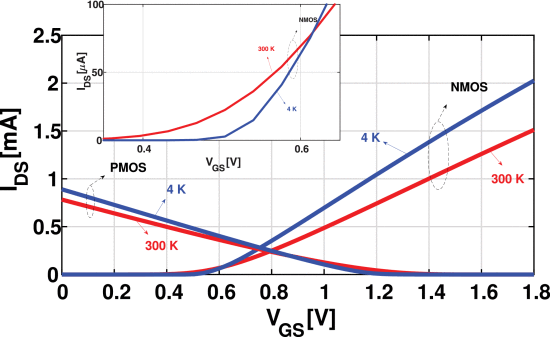
# *Figure 2- Output characteristics of (a) thick-oxide and (b) thin-oxide NMOS and PMOS in 160-nm CMOS technology.*

[Figure 4](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/4/8241022/8036394/patra4ab-2737549-large.gif)

****

# *Figure 3-Output characteristics of (a) thick-oxide and (b) thin-oxide NMOS and PMOS in 40-nm CMOS technology.*

[Figure 5](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/4/8241022/8036394/patra5-2737549-large.gif)



# *Figure 4- ID –VG characteristic of thin-oxide NMOS and PMOS in 160-nm CMOS technology. Inset: clear shift in threshold voltage for the NMOS characteristics*.

The cryogenic behaviour of other devices, such as resistors and substrate BJTs, also deviates from that at 300 K. Carrier freeze-out is evident in the increase of the n-well resistance by several orders of magnitude at 4 K (Fig. 6). Better temperature stability is achieved by other types of resistors, such as N-poly (±10%) and P-active (±20%). Parasitic substrate pnp BJTs are usually employed in bandgap references and temperature sensors, but their behaviour deteriorates below 70 K due to freeze-out in the base.

Significant changes are also observed in digital logic. Despite the drawbacks related to the higher threshold voltage, digital logic benefits from the higher *I*ON/*I*OFF ratio due to the steeper sub-threshold slope. The measured delay of an inverter in 160-nm CMOS at a nominal supply voltage improves by 20%, from 38.3 ps at 300 K to 30.6 ps at 4 K. In 40-nm CMOS, the improvement is 36%, indicating that significant speedups can be achieved at cryogenic temperatures.

1. **Advantages and disadvantages of quantum computer**

**Advantages of Quantum Computing**:

* The main advantage of quantum computing is it can execute any task very faster when compared to the classical computer, generally the atoms changes very faster in case of the traditional computing whereas in quantum computing it changes even more faster. But all the tasks can’t be done better by quantum computing when compared to traditional computer.
* In quantum computing qubit is the conventional superposition state and so there is an advantage of exponential speedup which is resulted by handle number of calculations.
* The other advantage of quantum computing is even classical algorithm calculations are also performed easily which is similar to the classical computer.

**Disadvantages of Quantum Computing:**

* The main disadvantage of computing is the technology required to implement a quantum computer is not available at present. The reason for this is the consistent electron is damaged as soon as it is affected by its environment and that electron is very much essential for the functioning of quantum computers.
* The research for this problem is still continuing the effort applied to identify a solution for this problem has no positive progress.

**7.Applications**

**7.1 Artificial Intelligence**

A primary application for quantum computing is artificial intelligence (AI). AI is based on the principle of learning from experience, becoming more accurate as feedback is given, until the computer program appears to exhibit “intelligence.”

This feedback is based on calculating the probabilities for many possible choices, and so AI is an ideal candidate for quantum computation. It promises to disrupt every industry, from automotive to medicine, and it’s been said AI will be to the twenty-first century what electricity was to the twentieth.

For example, Lockheed Martin plans to use its D-Wave quantum computer to test autopilot software that is currently too complex for classical computers, and Google is using a quantum computer to design software that can distinguish cars from landmarks. We have already reached the point where AI is creating more AI, and so its importance will rapidly escalate.

**7.2 Molecular Modeling**

Another example is precision modeling of molecular interactions, finding the optimum configurations for chemical reactions. Such “quantum chemistry” is so complex that only the simplest molecules can be analyzed by today’s digital computers.

Chemical reactions are quantum in nature as they form highly entangled quantum superposition states. But fully-developed quantum computers would not have any difficulty evaluating even the most complex processes.

Google has already made forays in this field by simulating the energy of hydrogen molecules. The implication of this is more efficient products, from solar cells to pharmaceutical drugs, and especially fertilizer production; since fertilizer accounts for 2 percent of global energy usage, the consequences for energy and the environment would be profound.

**7.3 Cryptography**

Most online security currently depends on the difficulty of factoring large numbers into primes. While this can presently be accomplished by using digital computers to search through every possible factor, the immense time required makes “cracking the code” expensive and impractical.

Quantum computers can perform such factoring exponentially more efficiently than digital computers, meaning such security methods will soon become obsolete. New cryptography methods are being developed, though it may take time: in August 2015 the NSA began introducing a list of quantum-resistant cryptography methods that would resist quantum computers, and in April 2016 the National Institute of Standards and Technology began a public evaluation process lasting four to six years.

There are also promising quantum encryption methods being developed using the one-way nature of quantum entanglement. City-wide networks have already been demonstrated in several countries, and Chinese scientists recently announced they successfully sent entangled photons from an orbiting “quantum” satellite to three separate base stations back on Earth.

**7.4 Financial Modeling**

Modern markets are some of the most complicated systems in existence. While we have developed increasingly scientific and mathematical tools to address this, it still suffers from one major difference between other scientific fields: there’s no controlled setting in which to run experiments.

To solve this, investors and analysts have turned to quantum computing. One immediate advantage is that the randomness inherent to quantum computers is congruent to the stochastic nature of financial markets. Investors often wish to evaluate the distribution of outcomes under an extremely large number of scenarios generated at random.

Another advantage quantum offers is that financial operations such as arbitrage may require many path-dependent steps, the number of possibilities quickly outpacing the capacity of a digital computer.

**7.5 Weather Forecasting**

NOAA Chief Economist Rodney F. Weiher claims that nearly 30 percent of the US GDP ($6 trillion) is directly or indirectly affected by weather, impacting food production, transportation, and retail trade, among others. The ability to better predict the weather would have enormous benefit to many fields, not to mention more time to take cover from disasters.

While this has long been a goal of scientists, the equations governing such processes contain many, many variables, making classical simulation lengthy. As quantum researcher Seth Lloyd pointed out, “Using a classical computer to perform such analysis might take longer than it takes the actual weather to evolve!” This motivated Lloyd and colleagues at MIT to show that the equations governing the weather possess a hidden wave nature which are amenable to solution by a quantum computer.

Director of engineering at Google Hartmut Neven also noted that quantum computers could help build better climate models that could give us more insight into how humans are influencing the environment. These models are what we build our estimates of future warming on, and help us determine what steps need to be taken now to prevent disasters.

The United Kingdom’s national weather service Met Office has already begun investing in such innovation to meet the power and scalability demands they’ll be facing in the 2020-plus timeframe, and released a report on its own requirements for exactable computing.

**7.6 Particle Physics**

Coming full circle, a final application of this exciting new physics might be… studying exciting new physics. Models of particle physics are often extraordinarily complex, confounding pen-and-paper solutions and requiring vast amounts of computing time for numerical simulation. This makes them ideal for quantum computation, and researchers have already been taking advantage of this.

Researchers at the University of Innsbruck and the Institute for Quantum Optics and Quantum Information recently used a programmable quantum system to perform such a simulation. Published in Nature, the team used a simple version of quantum computer in which ions performed logical operations, the basic steps in any computer calculation. This simulation showed excellent agreement compared to actual experiments of the physics described.

“These two approaches complement one another perfectly,” says theoretical physicist Peter Zoller. “We cannot replace the experiments that are done with particle colliders. However, by developing quantum simulators, we may be able to understand these experiments better one day.”

Investors are now scrambling to insert themselves into the quantum computing ecosystem, and it’s not just the computer industry: banks, aerospace companies, and cybersecurity firms are among those taking advantage of the computational revolution.

While quantum computing is already impacting the fields listed above, the list is by no means exhaustive, and that’s the most exciting part. As with all new technology, presently unimaginable applications will be developed as the hardware continues to evolve and create new opportunities.

**8. Commercial Quantum Computer**

The company D-Wave Systems has been offering what they call quantum computers commercially since 2011. Many things seem to point towards those being adiabatic quantum computers (though people disagree on this). That doesn't quite fit the kind of quantum computers that are becoming popular right now though. There is still a search for problems where the D-Wave shows improvement over classical algorithms. There is some evidence that there are indeed some quantum effects used by the D-Wave. On the other hand, there have been a few papers on the topic of the D-Wave being a simple thermal annealer with no quantum effects, although they are a bit dated now.

Companies such as IBM in the other hand are offering access to circuit model quantum computers (with physical qubits). IBM specifically does this in the IBM Q project via their website and a programming interface. They cooperate with commercial companies to explore possibilities in the quantum computing field. (A similar offer is available from Rigetti Computing via their Rigetti Forrest project.) That's not what most people would call "commercial quantum computers" though.

**9.Conclusion**

With classical computers gradually approaching their limit, the quantum computer promises to deliver a new level of computational power. With them comes a whole new theory of computation that incorporates the strange effects of quantum mechanics and considers every physical object to be some kind of quantum computer. A quantum computer thus has the theoretical capability of simulating any finite physical system and may even hold the key to creating an artificially intelligent computer.

The quantum computers power to perform calculations across a multitude of parallel universes gives it the ability to quickly perform tasks that classical computers will never be able to practically achieve. This power can only be unleashed with the correct type of algorithm, a type of algorithm that is extremely difficult to formulate. Some algorithms have already been invented; they are proving to have huge implications on the world of cryptography. This is because they enable the most commonly used cryptography techniques to be broken in a matter of seconds. Ironically, a spinoff of quantum computing, quantum communication allows information to be sent without eavesdroppers listening undetected.

For now, at least, the world of cryptography is safe because the quantum computer is proving to be very difficult to implement. The very thing that makes them powerful, their reliance on quantum mechanics, also makes them extremely fragile. The most successful experiments only being able to add one and one together. Nobody can tell if the problems being experienced by researchers can be overcome, some like Dr. Gershenfield are hopeful that they can whilst others believe that the quantum computer will always be too fragile to be practical.

**10.REFERENCES**

* L. Vandersypen, "Quantum computing—The next challenge in circuit and system design", *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, pp. 24-29, Feb. 2017.
* F. Sebastiano et al., "Cryo-CMOS electronic control for scalable quantum computing: Invited", *Proc. 54th Annu. Des. Autom. Conf. (DAC)*, pp. 13-1-13-6, 2017.
* T. J. Green, J. Sastrawan, H. Uys, M. J. Biercuk, "Arbitrary quantum control of qubits in the presence of universal noise", *New J. Phys.*, vol. 15, no. 9, pp. 095004, 2013.
* Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In 35th Annual Symposium on Foundations of Computer Science. IEEE Press.
* Narayanan, A. and Moore, M. (1996). Quantum inspired genetic algorithms. In Proceedings of the 1996IEE International Conference on Evolutionary Computation (ICEC96). IEEE Press.
* Chen Jilian, Wang Lingli, Wang Bin, "Quantum FPGA Architecture Design", *IEEE*, 2013.
* Usman Khalid Ahmed, Zilic Zeljko, Radecka Katarzyna, "FPGA Emulation of Quantum Circuits", *Proceedings of the IEEE International Conference on Computer Design*, 2004.
* The Research of Grover’s Quantum Search Algorithm with Use of Quantum Circuits QX2 and QX4. Information Systems Architecture and Technology: Proceedings of 39th International Conference on Information Systems Architecture and Technology – ISAT 2018
* D. P. DiVincenzo, J. Smolin, "Results on two-bit gate design for quantum computere", *IEEE Workshop on the Physics of Computation.*
* L. Song, H. Homulle, E. Charbon, F. Sebastiano, "Characterization of bipolar transistors for cryogenic temperature sensors in standard CMOS", *Proc. IEEE SENSORS*, pp. 1-3, Oct. 2016.