"Quantum Computing" Future of computing

Prince Chopra
Research Scholar: B.Tech 4th year (Computer Science)
Maharaja Surajmal Institute of Technology (GGSIPU), Delhi, India
chopra0@gmail.com

Rachit Tomar
Research Scholar: B.Tech 4th year (Computer Science)
Maharaja Surajmal Institute of Technology (GGSIPU), Delhi, India
tomarrachit16@gmail.com

Mayank Bajaj
Research Scholar: B.Tech 4th year (Computer Science)
Maharaja Surajmal Institute of Technology (GGSIPU), Delhi, India
mayank_bajaj94@yahoo.in

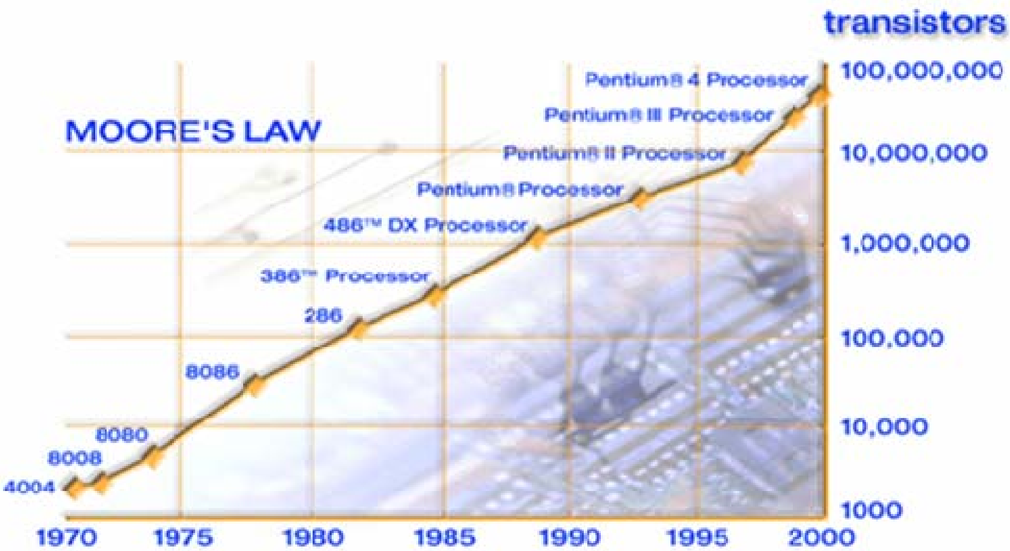
Abstract - Quantum computing studies theoretical computation systems (quantum computers) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. This paper will focus on the extent to which quantum computing will be helpful, will compare classical versus quantum computing and some problems which are not feasible to solve by classical computing which calls for a demand of faster computer which is Quantum Computer. The researcher's have discovered the possibility for an entirely new type of computer, one that operates according to the laws of quantum physics. A quantum computer would not just be a traditional computer built out of different parts, but a machine that would exploit the laws of quantum physics to perform certain information processing tasks in a spectacularly more efficient manner.

Keywords- Quantum Computing, Moore's Law, Classical versus Quantum computing

INTRODUCTION

It is not very difficult to note that computers are going faster by the day. One person that has been looking at the miniaturization of computers for the past several decades is Gordon Moore, the co-founder of Intel. Back in the 1960's, he noticed that the number of components on a silicon chip double roughly every eighteen months to two years.

Now if it's happening, it means that the smallest feature size on the silicon chip has to decrease at a similar rate, and he came out with something that is called Moore's law.



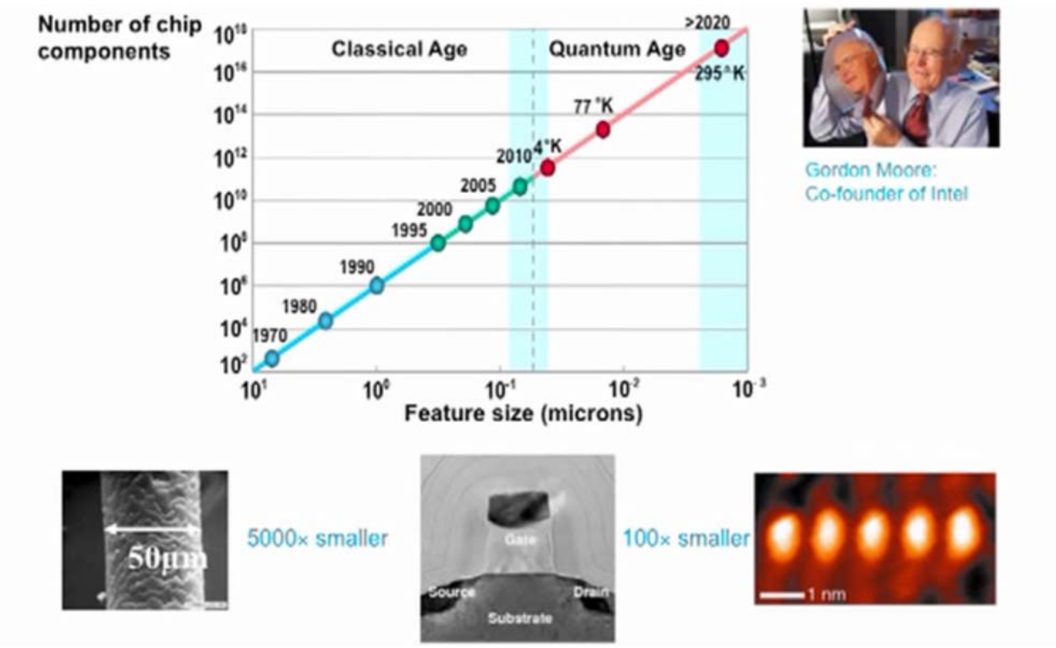
And this law has been going now for 5 decades, the sorted out as an observation by Gordon Moore's has became a law after his name. i.e. "Moore's law", it's actually continued in time.

The interesting thing is that industries have set this as a roadmap for how to make computers more and more fast. We now have multitrillion dollar semiconductor industries pouring in money, every year to beat that law, until now it has become a self-fulfilling prophecy!

What is Quantum Computing?

Quantum computing studies theoretical computation systems (**quantum computers**) that make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.[1] Quantum computers are different from digital computers based on transistors. Whereas digital computers require data to be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits (qubits), which can be in superposition's of states.

MOORES LAW TO ATOMIC SCALE



Smallest feature size in this transistor is the distance between source and the drain is 30 nm (i.e. 5000 times smaller than the width of human hair). What is amazing about that is if we look around now, we all carry around our personal electronics and within 1 silicon chip we have 3 billion of these transistors, and they all have to work reliably so that our electronics we are carrying should actually work.

One of the nice things about Moore's law is that we can predict with time what is going to happen. Eventually, we can see in that above image that in roughly 2020, the size of the transistors will be approximately equal to the size of an atom. Too difficult to imagine that we can make transistors any smaller than that.

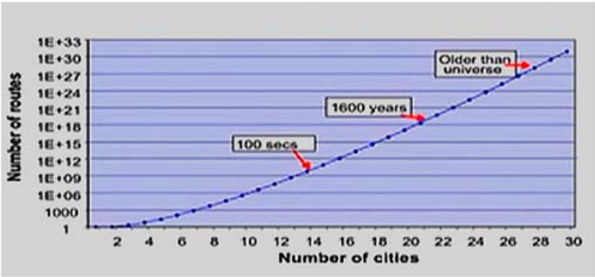
Everything we work around is coded in binary. What happens when we go smaller and smaller in size? We actually crossover from the classical age to the quantum age, and there things really start to change.

In the classical world, we understand how things work. Let's say we have a tennis ball and we throw it towards the wall and it bounces back and we will understand the equations used to describe that.

If we miniaturize things, and imagine that tennis ball is the electron in our transistor, and we threw that electron at the wall, instead of it bouncing back, it actually behaves more like a wave than a particle and it will travel through the wall & come out the other side. That something that is quite scary. As we make our devices smaller and smaller the wonderful world of quantum mechanics comes in. Electrons will behave like wave particles and they no longer go in the computer where we want them to go. So most of the people have predicted that this will herald the end of Moore's law. But in reality it is the start of something new. We are now transitioning into quantum mechanics. If we control quantum physics, we can actually build the computers in quantum regime. We are predicted to have exponential speedup of our classical computers. People are of the opinion that aren't our computers fast enough to do all the things that we want them to do. But there are some problems out there that just can't be solved efficiently using a classical computer.

TRAVELLING SALESMAN PROBLEM

A salesman has to travel to many cities and wants to work out the shortest possible route



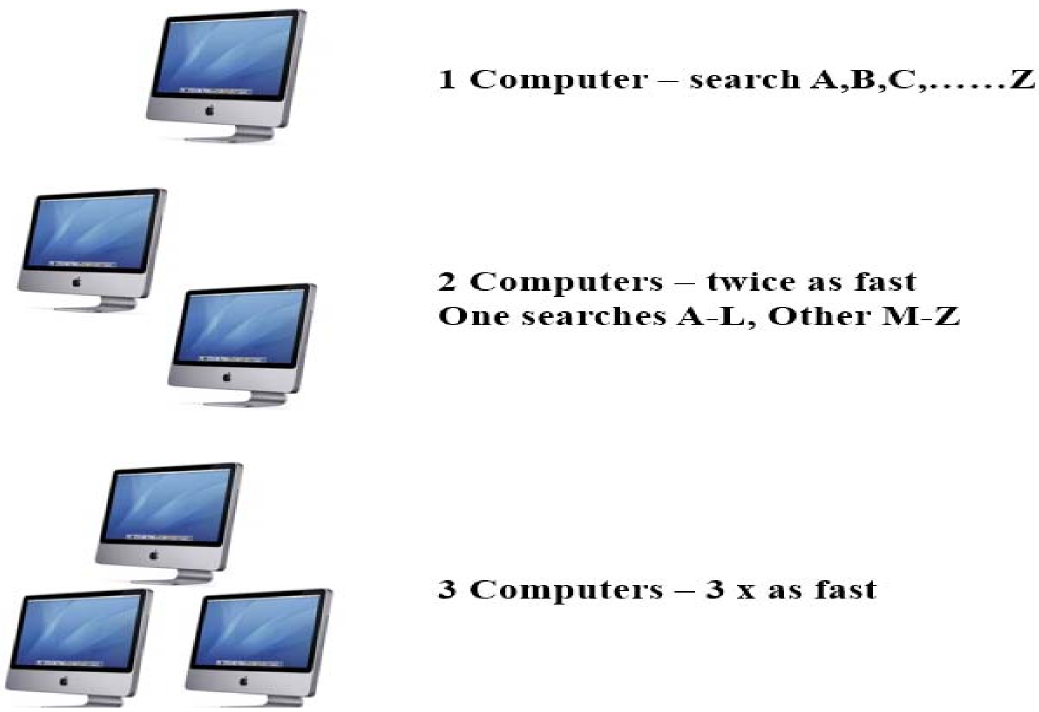
14 Cities: 10^11 Routes
For a classical 1GHz computer (10^9 operations/sec)
It would take 100 seconds

22 Cities: 10^19 Routes
It would take 1600 years

For 28 cities it would take time older than the universe

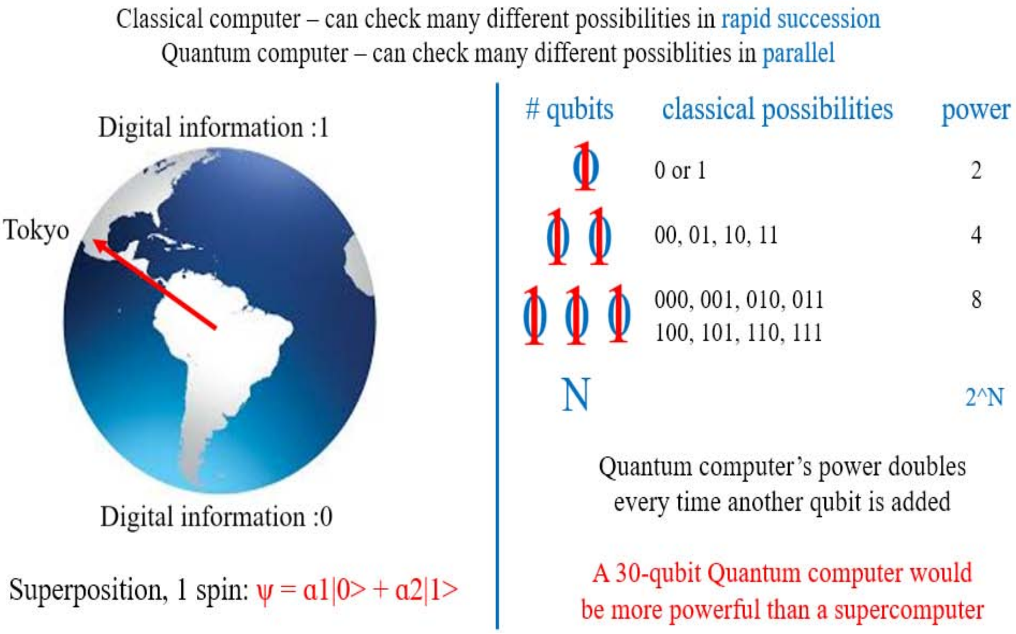
This is one of the intractable exponentially hard problems i.e. number of possible routes he can take as a function of number of cities, something that grows very quickly. For the time, we have 14 different cities and there are already 10^11 possible routes he can take. If we take a classical computer that works in gigahertz regime, then it can work out the smallest possible route in 100 seconds. But now what happens when we go for 22 cities. There are, now, 10^19 possible routes that he can take (and with the same classical computer, it would take 1600 years).And if we look by 28 cities, it would take longer than the lifetime of the universe to work out what is the shortest possible route is. The fact is that it is a real problem that exists out there. So, how can we make a computer that somehow solves those kinds of problems? Let's have a look at how a classical computer works. A classical computer is very fast. It searches the entire possibilities.

So if we have to write down a telephone number on a piece of paper and we'd forgotten whose telephone number it is, then our classical computer will start looking through all the A's then all the B's so on , and eventually finds whose number it is and tells us. If we wanted to go faster, we will put two computers onto the problem (one searches from A-L and other M-Z), and even faster with 3 computers.



If we could make a quantum computer, the actual calculation is done in parallel and simultaneously. Let's understand these things.

CLASSICAL VERSUS QUANTUM COMPUTATION



In case of a classical computer. : - Imagine we are sitting at the centre of the earth and we are pointing towards the North Pole (let's assume it as '1' of digital information) or we could be pointing at the South Pole (that's the '0' of digital information)

In case of quantum comp.:- In the quantum world we could be pointing anywhere on the surface of earth and which can be explained with the superposition equation showing us partly up and partly down. In the quantum world we can be in both states at the same time.

How does that help me in calculations?

Look when we increase the number of quantum bits or qubit's, for 1 qubit equals 2 possible states at same time; if we add 2 qubit's equals 4 possible states at a time and so on.

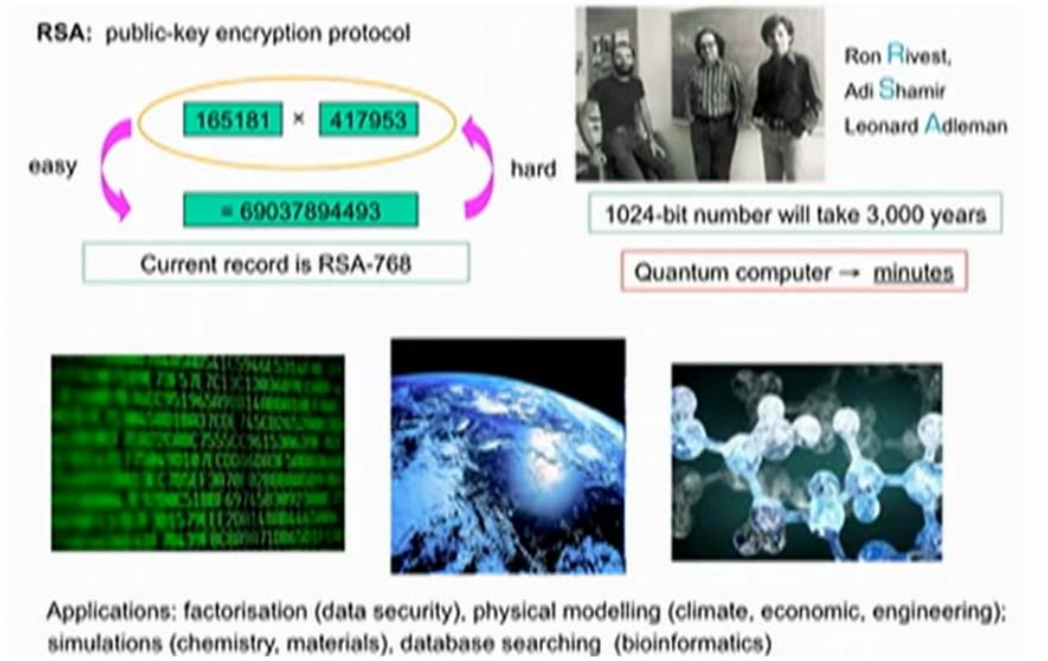
Every time we add a quantum bit, we double the computational power of the quantum computer. So, it is predicted that the 30 qubit quantum computer is more powerful than the world's most powerful supercomputer that exists. If we have 300 qubit's in quantum computer, then it will be more powerful than all the computers in the world combined together.

That suggests 300qubits compared to 3 billion conventional transistors, that's really the power of quantum computation.

PROBLEMS ASSOCIATED

Let's consider some of the problems that quantum computers can solve for us. One of the things that people realize is that it could actually be useful for data encryption. The data encryption relies on working out of prime factors of large numbers. E.g.: If we have 2 prime factors, if we times these 2 numbers together which is very easy for computer but if we want to get prime factors of a large number, it will be hard. So, we can give one prime factor as a key so that it can be decoded at the other side. If they don't have the key though, the work for the prime factor will be very difficult.

WHAT CAN QUANTUM COMPUTERS DO?



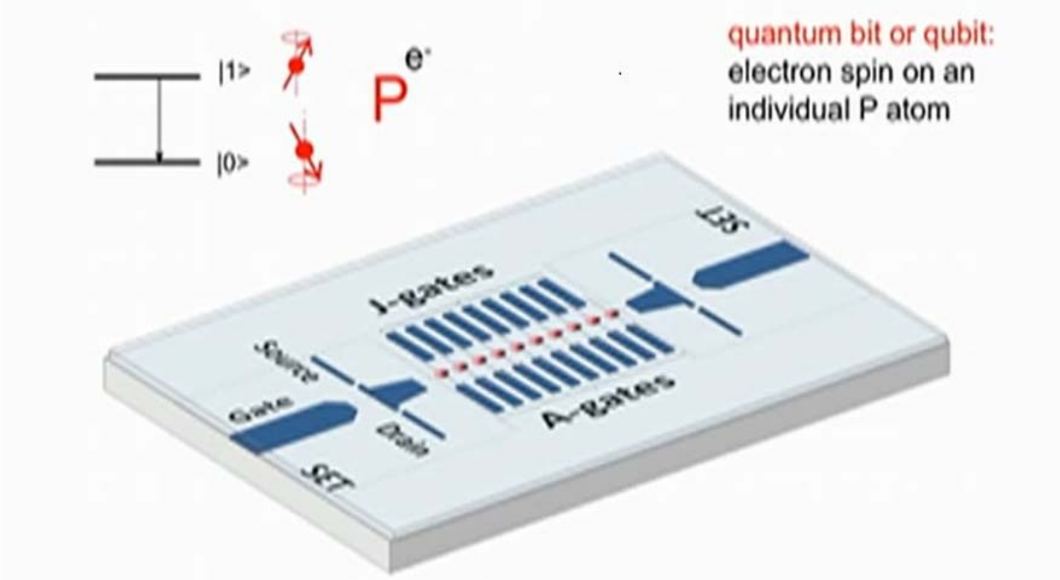
Very recently they have broken the code in 2007i.eRSA-768. It is a 768 bit number. It took 3 years using the most powerful classical computers that exist. Now, they are encoding 1024 bit number using the same classical computers it will take 3000 years. If we had a quantum computer it could solve it in minutes.

Data security is another thing at which quantum computers are greater is searching large database or large amount of information for modelling systems with lots of variables. We could start imagining climate modelling. We could start imagining how chemicals form, how new things starts evolving and how human body forms. With quantum computation, it can take us to something we don’t know, that’s a huge potential. So as a consequence there is a massive international race to build the quantum computer.

SILICON IS GREAT FOR IT

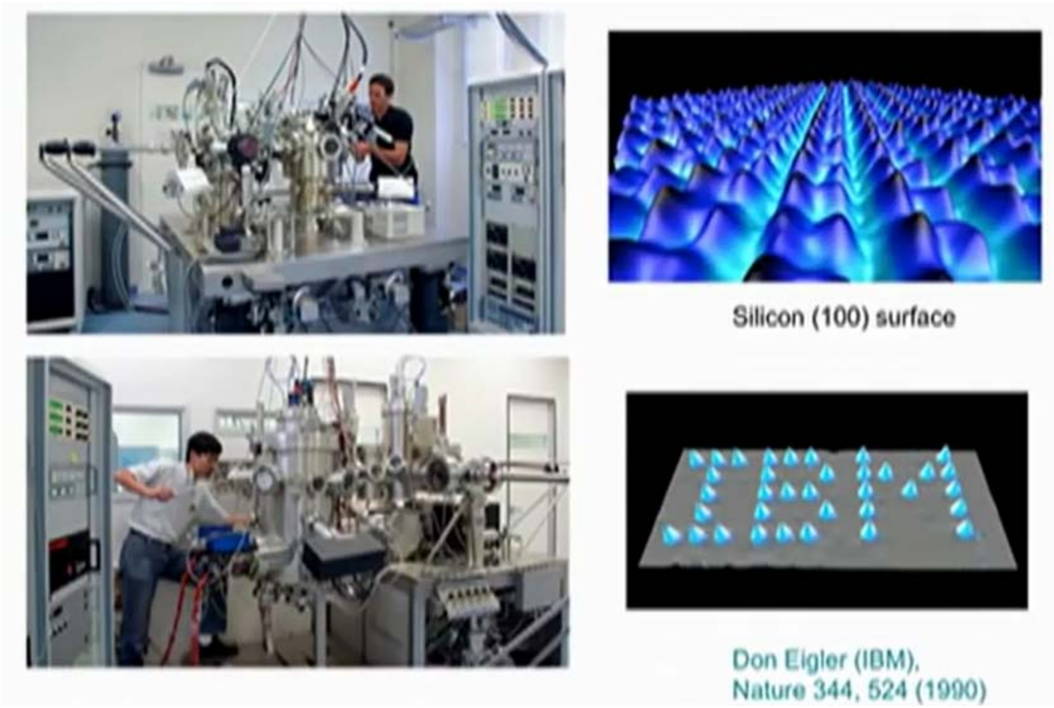
Let’s consider Silicon. Now, the reason why we've chosen silicon is it's one of those great materials. The industry has been using it for years. If we want to make a quantum computer in silicon, we have to engineer single atoms. Not just the single atom, but also the individual electron on a single atom, in silicon, and encode our information in that quantum bit or qubit. Silicon's great, because the industry has been working on it for years. But it means that we're going to be pushing the end of Moore’s law to make those single-atom transistors. Silicon's also great because it's a material that doesn't interact with the electrons. It's a nice pure host material to protect that fragile quantum state.

QUANTUM COMPUTER USING SINGLE ATOM QUBITS



To realize this quantum computer, we have to put these individual atoms in position within a silicon crystal and then we have to align electrodes to that single atom which means everything has to be incredibly small. Well, how do we image or manipulate atoms? The only technology that exists out there is a scanning tunnelling microscope. This is something that has a very fine metal tip that it brings down to atom's surface. When we bring it down very close, we apply a voltage and we get a current. And what we try and do is keep that current constant and move the tip over the atom. And as it moves, it deflects in height. From that, we can actually image the atoms on a surface. Then we raster-scan it, rather like a television screen. We can build up an image of what the atoms looks like on the surface.

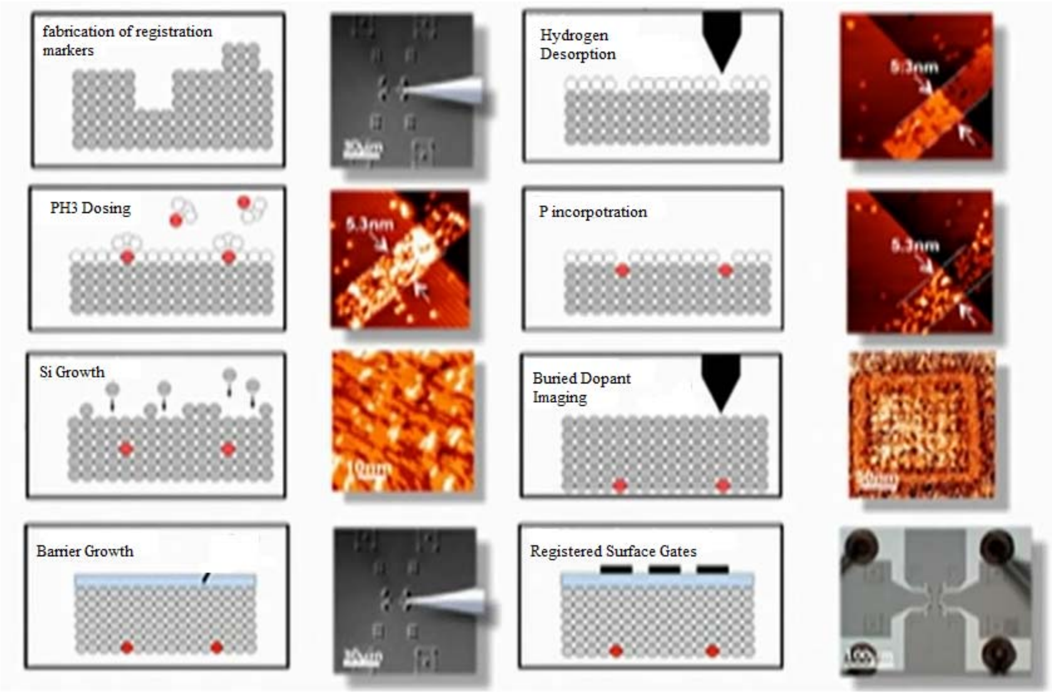
SINGLE ATOM IMAGING AND MANIPULATION



Now, we are blown away by this image. These are individual silicon atoms sitting on the silicon surface that transistors are made on. That's really phenomenal. Now, we might imagine the machinery that we use to image those atoms is very small, just a very small tip. But in reality this is what it looks like. They're very large systems; they take up about the size of a room. They're basically huge chunks of stainless steel with a very high vacuum inside. Rather like the vacuum that we find in outer space. And within that vacuum we put samples in and we control the atoms and we have mechanical, pumping and electronic control to be able to image those atoms on the surface. But we can also connect them here with crystal growth systems where we can actually put different atoms on the surface. So we can actually create new materials that just don't exist in nature. To give us an idea of one of those, here's the world's smallest logo. These are xenon atoms on a copper surface. It was done in the1990'sby the IBM group by Don Eigle. Literally, they used that tip to pick up individual atoms and put them down to form the world's smallest logo. Well, what we want to do now is to make devices in silicon using this technology. But it's not as easy as just manipulating atoms on the surface.

There's two key problems. The first one is that we can only see the device inside these systems, these microscopes. We can't see them once we take them outside. So, we've had to develop that technology. The second one is that we can't just manipulate atoms in silicon very easily.

RADICAL ATOMIC-SCALE FABRICATION STRATEGY

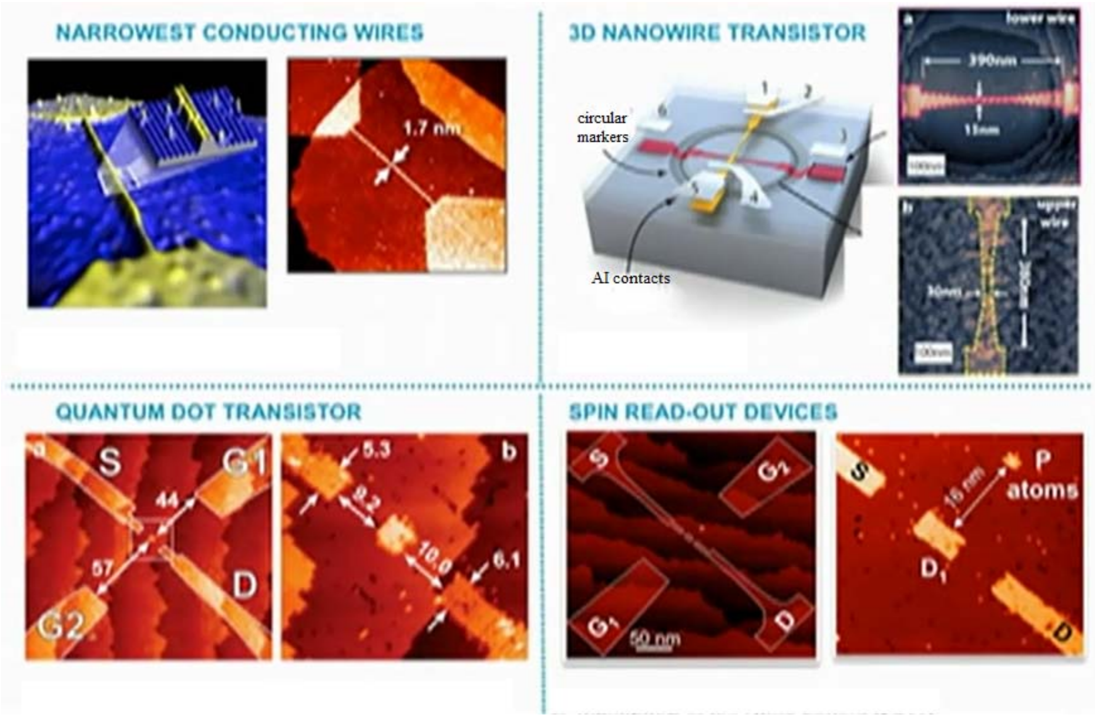


They actually bond very strongly together. So, as a consequence, we had to come up with a radical strategy to build these devices. The first thing we do is we have to make a marker in the silicon substrate before we put it into those systems. We then take it in there and we put down a layer of hydrogen on the surface. And this layer of hydrogen acts as a mask. We're going to come along with our scanning probe tip and dissolve some hydrogen. Thereby, exposing the silicon underneath. And this is how we're going to bring our atoms in. We dose with phosphine that brings our phosphorus atoms in.These are going to be our qubits and they only go in the regions that we've depassivated. We then incorporate them into the surface. We encapsulate them with silicon so they're nice and robust. And we can actually go back and image them at this point and show that they haven't moved. And then once we've done this, we take it out of the vacuum system. We use those registration markers to bring down metal contacts to the device.

So when we first presented this proposal about ten years ago, people said," None of that's been realized. Each one of those strategies incredibly hard to do. "But, Australia, over the last ten years, has actually started making these devices. And systematically building bit by bit those components of a quantum computer, they've made very narrow conducting wires, one atom tall and four atom wide. They're very similar to the copper wires that we have in conventional transistors. They've made the smallest precision transistors, where they've been able to watch individual electron shop on and off an island. They've been able to move to three-dimensional architectures, and for us, this is amazing.

All the transistors we have at the moment, all the electrons travelling one two-dimensional plane. We don't use the Z direction at all. So we've found a way that we can actually make vertical transistors. And this is something we're going to use for our quantum computer architecture. And also very recently we've been able to isolate a few of these phosphorus atoms and we've actually used another transistor patterned nearby to actually measure the electron spins so we can read out the quantum states in our quantum computer.

BUILDING DEVICES ATOM BY ATOM



But perhaps one of the most difficult challenges for us today has been to isolate a single atom in a device. And just last year we were able to form the world's first precision single atom transistor. So that really is an individual phosphorus atom sitting in the silicon substrate, where we've aligned these electrodes to it, taken it out of the vacuum system and made contact to it. We can actually measure the electronic signature of that single atom directly.

So rather like the human beings in this audience, we each have a well-defined identifiable fingerprint; a single atom also has a well-defined identifiable fingerprint. And this is what the electronic fingerprint of that single atom is. The amazing thing about this is we could change the atom, and we'd get a completely different fingerprint .So it really is unique. So what we've demonstrated over the last decade, and we're leading this field in Australia, is we can make devices out of single atoms. This has taken us all the way down to the end of Moore’s law.

So the question now is, "Is that the end of computing?”. Instead of miniaturizing transistors over the last 50 years, we're now going to start from the bottom and we're now going to start to build quantum computers where we add individual qubits one at a time. Every time we add a qubit, we double the computational power. So that's the international race to try and build a large-scale quantum computer that can do calculations we simply cannot do with a classical computer.

REFERENCES

[1] “Quantum Computing” Available at: https://en.wikipedia.org/wiki/Quantum_computing
[2] “Quantum Computers & Moore's Law” Available at: https://www.qubyte.com/
[3] Manay, K. (1998). “Quantum computers could be a billion times faster than Pentium III.” Available at: https://www.amd1.com/quantum_computers.html/
[4] “Quantum Computers: What are They and What Do They Mean to Us?” Available at: https://www.carolla.com/quantum/quantumcomputers.htm/
[5] M. Nielson, I. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, Cambridge, 2000).