

THE 2008 CAP CONGRESS HERZBERG LECTURE: HARNESSING THE QUANTUM WORLD

BY RAYMOND LAFLAMME AND JEREMY CHAMILLIARD

Humans are curious, perhaps because of our survival instinct or perhaps because we have realised that we can make our lives more comfortable with the fruits of curiosity. This curiosity leads us to examine natural phenomena and to attempt to understand them. With some understanding, we can control these phenomena and turn them into the basis for new technologies. Over the course of human history we have seen this repeated cycle of discovery, understanding, controlling and leveraging phenomena for technologies that have profound impacts on societies.

An example of this cycle is the harnessing of fire. Many thousands of years ago, fire was discovered after lightning storms set forests ablaze. We learned to control fire in a pit surrounded by stones and eventually to use it to make tools both for hunting and for agriculture. Agriculture allowed us to form settlements, profoundly changing our

INTRODUCTION TO HERZBERG LECTURE

It is a great pleasure for me to give the Herzberg lecture, opening the 2008 Canadian Association of Physicists Congress at the Université Laval. Before I delve into the quantum world, I would like to thank the committee who have chosen me to give this lecture. It is also a great honor for me to have been introduced by René Roy, as he was a mentor to me. In 1981, I was a summer student here in Québec working in nuclear physics with Professor Roy. At that time, I could never have imagined that 27 years later I would be giving this lecture. I am also moved to give a lecture in the honour of Dr Gerard Herzberg, who has inspired a generation of Canadians. Finally, it is interesting to reflect on being here in Québec 400 years after its foundation. Only 100 years before that, John Cabot had just discovered Canada. That was an exciting time of discovery and exploration of a new world. Today, 100 years after the discovery of quantum mechanics, the first institutes to study quantum information processing are being founded and starting to explore the richness of the quantum world. I wonder what the field will look like 400 years from now.

everyday lives. Thousands of years later, we observe another of these cycles in the harnessing of steam power. Initially, steam was observed as a phenomenon that occurred when water was boiled, perhaps for cooking. However, once harnessed, steam power started the industrial revolution, allowing us to make not only new tools, but also tools which could make tools themselves. It also enabled steam engines and the locomotive providing the ability for humans to travel further than ever before. Again this brought a drastic change to our society, connecting towns and cities and bringing nations together. Another, more recent example has been harnessing the forces of electricity and magnetism discovered by Faraday and others. These forces were unified through the work of Maxwell and over the past 100 years we have learned to control these forces, leading to the information revolution that is still happening today. From \$5 dollar watches to multi-billion dollar satellites, our society has undergone a revolution to one where information processing devices are pervasive. Our children can no longer imagine what life would be like without these devices. They are critical for everything from scientific research, to the way we entertain ourselves, to the economy of the world. These devices have allowed us to build computers that are now ubiquitous and communication devices that allow our daily interaction to expand from cities to the entire planet. They are not only changing the way we behave but ultimately, I believe, they are changing the way we think and are redefining who we are. Observing, learning, controlling and turning natural phenomena into technology is part of our history. The question is, what is the next natural force or effect that we will harness and transform both our technological world and our society?

The information revolution has been possible over the past 50 years because we have become extremely good at manipulating larger and larger amounts of information, making information processors more and more powerful. How did we do this? To explain, I will not focus on the meaning or the implication of the information itself but more on how it is encoded and manipulated. In this description, it suffices to think of information processing devices as physical systems that manipulate bits of information. The bits are the basic units of information, and can be encoded in systems that have two states, labelled 0 and 1. For example, a capacitor that is either charged or discharged, or a magnet pointing up or down. All information that we need to use and manipulate can be translated



R. Laflamme
<laflamme@iqc.ca>,
Institute for Quantum
Computing,
University of
Waterloo, Waterloo
ON, N2L 3G1

and

J. Chamilliard,
Institute for Quantum
Computing and Dept
of Physics and
Astronomy, University
of Waterloo, Waterloo
ON



into strings of bits. The letters of the alphabet, decimal numbers, pictures from a camera and instructions for a computer program can all be transformed into strings of bits. To communicate, we send strings of bits between parties, and to compute, we manipulate one bit string into another. If necessary, some software or hardware can translate the bit strings back to text, sound or graphics. Today, all these manipulations are done using the so-called laws of classical physics—the laws inherited from the Galileo, Newton, Maxwell and other pioneers.

When electronic computers started to be built in the late 1940's, users quickly realised that the machines were never powerful enough to do what they really wanted them to do. Two strategies were used to improve the technology: simplify the problems so that they could be managed with the available devices; or try to make the devices more powerful. How do we make information processing devices more powerful? A simple answer is to make them faster so that they can manipulate more information in the same amount of time.

A related question is, what limits our ability to manipulate information? Physicists like Richard Feynman, asked: What are the fundamental limitations to information processing due to the laws of physics? An example of a limitation is the fact that Einstein's theory of special relativity gives a maximum speed at which a signal can be transmitted, placing an upper limit on the speed of an information processor. The time it will take to communicate bits of information must be at least the distance they must travel divided by the maximum speed of transmission—the speed of light. Another question he asked was, is there a fundamental limit to the size of the physical system that can encode bits? In the 1960's, Rolf Landauer suggested that due to a certain amount of heat that must be dissipated for any information processor to process data, it will have a minimum size beyond which it will not be possible to remove the heat generated. Yet another question posed by Feynman was, what will the influence of quantum effects be on information processing? This will be revisited later.

One method of making information processors faster is to bring the physical systems that encode the bits closer to each other which can be done by compacting the entire device. This is indeed the approach that has been used by the computing industry for the past 50 years. In the early 1970's, Gordon Moore, then chairman of Intel, noticed that engineers were able to shrink transistors enough to pack twice as many per unit area about every 18 months. His suggestion that this pace would continue is now known as Moore's Law. Initially, nobody took Moore's Law seriously, but engineers kept on the target during the 70's, the 80's, the 90's and even up to today in 2008. In the 1950's, the first transistors were the size of centimeters; today they are merely tens of nanometers. This is an amazing feat of engineering that I would even compare to building the Pyramids of Egypt. If this pace keeps up, transistors will be the size of atoms in the next 10 to 15 years. As we proceed towards that scale, the laws of physics change; the

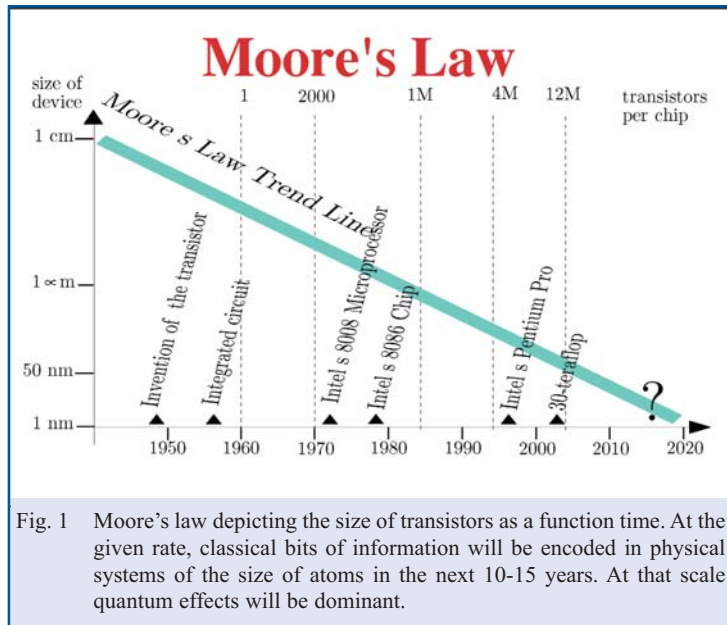


Fig. 1 Moore's law depicting the size of transistors as a function time. At the given rate, classical bits of information will be encoded in physical systems of the size of atoms in the next 10-15 years. At that scale quantum effects will be dominant.

classical laws do not accurately describe the system and are instead replaced by the laws of quantum mechanics. Quantum effects have already appeared in recent generations of chips, but clever engineering has mitigated their effects. From this point of view, quantum mechanics seems like an obstacle to what we have been incredibly good at for the last 50 years. However, from a different perspective, we may be able to turn things around and change the rules of the game. We may be able to use these laws of quantum mechanics to our advantage for information processing. This is the goal of quantum information science. In fact what we have found in the last 10 to 15 years is that for certain problems it is much much better to process information with quantum mechanics than to use the classical laws.

Before going into detail on how we can use quantum rules to compute, let's briefly review quantum mechanics. The first phenomena making apparent the elements of quantum mechanics were observed at the beginning of the 20th century. It was known then that the classical theory of electromagnetism was not able to explain the spectrum of radiation inside a box with black walls at thermal equilibrium. What was observed in the spectrum was a rapid decrease in radiation intensity at short wavelengths contrary to the classically predicted increase. Planck was able to explain this phenomenon by postulating that radiation can only occur in discrete chunks of energy and not continuously as was the classical theory. Another phenomenon that was explained by quantizing electromagnetic waves was the photo-electric effect, observed by irradiating metallic plates with light. It was found that the light caused electrons to be ejected from the plates, however varying the intensity of the light did not change the velocity of the ejected electrons as expected. Moreover, there was a minimum frequency below which no electrons were ejected at all. This effect was explained by Einstein who postulated that light came in parcels

of discrete energy called photons. Finally, there was the puzzle of how atoms could be stable in the classical theory. In the planetary model of the atom, electrons circulate around the nucleus and thus by the classical laws, should emit radiation as they are accelerating. As the electrons emit radiation, they should lose energy and a rough calculation tells us that within about a nanosecond they should collapse on to the nucleus, obviously in contradiction with observation. Bohr suggested that only discrete orbits were allowed and electrons could take only discrete orbits corresponding to a full integer number of cycles of their waves. This had the added bonus of explaining that atoms would only radiate energy with discrete frequency values, something that had already been observed. Planck, Einstein and Bohr hypothesized that energy was packaged in discrete values instead of continuously in the classical theories. This was the basis of quantum mechanics and a new mathematical framework was created in the 1920's that explained the aforementioned phenomena. At the same time, this theory predicted new, unusual and counterintuitive phenomena. A glimpse of some of these unusual phenomena is provided by the so-called double slit experiment.

In 1806, Thomas Young devised an experiment that consisted of sending light through two slits and measuring the intensity on the other side projected onto a screen. The intensity observed when blocking the top slit is given by the green line in Figure 2, where the red line is given by blocking the bottom. However, if both slits are open the sum of the two previous results (the line in black) is not observed, but instead a more jagged line (in blue) revealing the phenomena of interference. This was explained by postulating that light behaves like a wave, similar to those on the surface of water. The slits behave like a source of waves and the fact that the pattern created by both slits open is different than the sum of the individual slits open can be understood as resulting from constructive and destructive interference of the waves. This description of wave optics was incredibly successful in the 19th century but challenges to the theory eventually arose.

At the beginning of the 20th century, it was noticed that the granularity of light does appear at low enough intensities; the light behaving as particles—the photons that were already mentioned. A revealing experiment uses the previously described double slit apparatus but with such low intensity of light so that only a single photon is in the apparatus at given time. When a single slit is open, the photon can pass through it and seems initially to appear randomly on the screen. However, after repeating with many photons, a pattern appears similar to the one obtained with the wave theory. Repeating the experiment with the other slit open gives the same pattern translated in space. The interesting results occur when both slits are open. Again the pattern initially appears random but eventually converges to the one predicted by the wave theory of light. How can there be interference from both waves if only a single photon is in the apparatus at a time? The explanation is that the laws of quantum mechanics allow the photon to be at more than one place at a time, in other words it can be in a superposition of more than one location. This seems preposterous from our classical

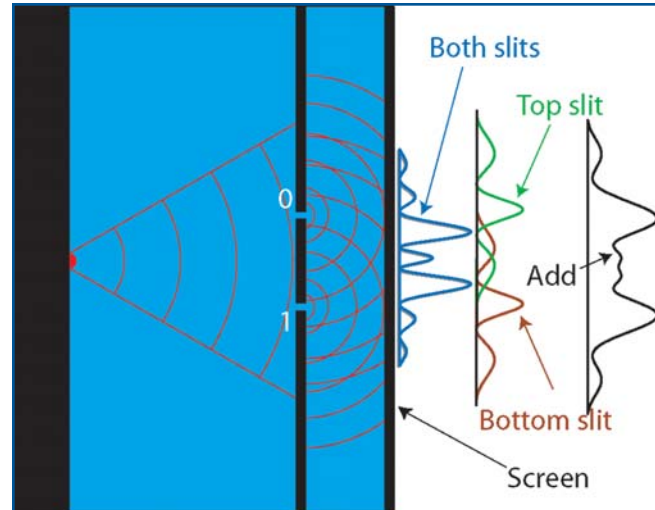


Fig. 2 The two slits experiment: light (in red) goes from the left to one or two slits and produce a pattern on a screen. When both slits are open, the resulting pattern is not the sum of the ones from individual slit but a new pattern appears coming from the interference coming for the combined effect of both slits. This interference pattern survive even when light intensity is so low that there is not more than a single photon in the apparatus at a given time, thus a single photon must have gone through both slits at once exhibiting the superposition of quantum mechanics.

conception of the world, nevertheless its consequence can be observed in this simple experiment. The ability to be in more than one state at thermal equilibrium is called the superposition principle of quantum mechanics and is an amazing property leading to many counterintuitive effects. It is the fundamental property used in quantum computers. Another unusual property of quantum mechanics that can be observed in the two slit experiments has a technological application. An astute observer could suggest that detectors be placed near the slits to learn through which slit the photon passes. Surprisingly, using a detector to observe this information destroys the interference pattern. This is another result of the theory of quantum mechanics which predicts quantum systems can not be observed without perturbing them. It turns out that this fundamental property can be used for what is called quantum cryptography.

The first quantum effect mentioned, the superposition principle, is useful for computing. Reusing the the double slit example, we assign the two states of the apparatus to a classical, computational bit. A photon passing through the top slit in the apparatus is assigned the bit value "0," and passing through the bottom slit is assigned "1". Since the system is quantum mechanical, it can also be both at once—a superposition of 0 and 1 at the same time. Now, imagine you have two bits. Two classical bits could be in one of the four states (00, 01, 10 or 11) but two quantum bits, called qubits, could be in all four states at the same time. Three qubits could be in a superposition of states (000, 001, 010,... 111). Ten qubits could be in a super-










# of quantum bits	superposition of the states	# of classical bits needed to simulate quantum states
1 	0,1	$2^1=2$
2 	00,01,10,11	$2^2=4$
3 	000,001,...,111	$2^3=8$
4 	0000,0001,...,1111	$2^4=16$
⋮	⋮	⋮
10 	0000000000,...	$2^{10}=1k$
20 	0000000000,...	$2^{20}=1M$
30 	0000000000,...	$2^{30}=1G$
40 	0000000000,...	$2^{40}=1T$
50 	0000000000,...	$2^{50}=1P$

Fig. 3 Quantum bits can be in a superposition of states. To simulate the evolution of a generic quantum computation with the best known classical algorithm using a classical devices would need an exponential number of classical bits.

position of 2^{10} , or about thousand states; 20 qubits, about a million states; and with 40 qubits a quantum computer could be in a trillion states—all at the same time. To simulate a quantum system of only 60 qubits using classical computers would require more resources than is available from every computer on the planet today. Concisely put, the power of the quantum computer is believed to be exponentially larger than their classical counterparts.

This exponential gain provided by quantum computation is revolutionary to computer science, as it challenges the so-called Church-Turing principle, a basic tenet of the field. The principle says that no machine could be exponentially more powerful than the traditional, classical computers used today. Many attempts have been made to get around the Church-Turing principle, however quantum computers are the first to pose a credible threat.

Another technology based on quantum effects is quantum cryptography, or to be more precise, quantum key distribution. Cryptography is the practice and study of information security. Here, we will focus on the secure transmission of information. Cryptography already has a classical way to exchange information with 100% security, called the “one time pad” or Vernam’s cipher. Two parties, call them Alice and Bob, can exchange perfectly secure information if they already share a ‘key’, or sequence of completely random series of bits—zeros and ones. The protocol works by Alice first translating a message into a string of bits and adding it to the key, creating an encoded message. The addition here is done through what is called a binary XOR operation—bitwise between the message string and the key. Explicitly, the XOR operation outputs a 0 if two bits have the same value, and 1 if they differ. The encoded string can then be sent to Bob who uses his copy of the key to perform the same operation, recovering the message. As the key is random, the encoded message will look random to anyone who does not

have the key, the basis of this security. An important point is that the key should not be reused as after observing many encoded messages, it may be possible for others to determine the key. The method using random keys is perfectly secure but the drawback is that Alice and Bob need to have previously met or at least exchanged the key in such a way so that an eavesdropper could not learn it. In highly secure application, such as for top-secret information exchange between embassies, diplomatic couriers are used. This is very inconvenient for instructing your bank to pay your credit card bill, however.

The security of the one time pad relies on the randomness of the key. In the 1970’s, mathematicians suggested methods where randomness was substituted for pseudo-randomness to increase the practicality of cryptographic schemes. Pseudo-random keys are keys that look random enough. They can be generated by mathematical problems that are hard to solve. An example of this is factoring numbers which are products of primes, like 15 (=5*3). Fifteen is relatively easy but factoring 2701 is a bit harder, and what about factoring 54029? It turns out that the best known classical algorithms take an amount of resources that grow as approximately $\exp(n^{1/3})$ where n is the number of digits of the number we need to factor. The cryptographic scheme that employs the factoring problem today is called RSA and works as follows: To securely transmit information to your bank on the internet, you first log in to their website. Next, the bank sends your computer a large number which is a product of two secret prime numbers. Your computer encodes your sensitive information using this large number and sends it to the bank. The bank can then decrypt the encoded information using the prime factors. The security of this scheme is based on the difficulty of solving a hard mathematical problem, in this case, factoring large numbers. Alarmingly, however, a quantum computer would have enough power to solve the types of problems that are used for today’s cryptography. Thus if transactions using the current methods are recorded, it might be possible to decode them in the future. Moreover, if a reasonable quantum computer could be built today, it would most certainly create havoc in the world of cryptography, such as that used for e-commerce. A quantum computer may not yet be a threat for our credit card numbers and financial transactions since the numbers will likely be changed before one can be built, but what about exchanging health care information on the internet today? The encoded information can be recorded today and decoded later if the technology becomes available. Quantum computing is already a potential threat to information that needs to remain secure for a long time.

It turns out that quantum mechanics can also protect information from quantum hacking. One of the weaknesses of classical cryptography is that in the classical world it is impossible to know if an eavesdropper is present. This is not the case in the quantum world. As mentioned previously, a quantum mechanical system can not be measured without perturbing it. This provides the opportunity to check if an eavesdropper is at work. With quantum cryptography, parties can exchange a key, check if an eavesdropper has intercepted it and if it was, throw away

the key and try again. Randomly sampling a small part of the key is sufficient to detect eavesdropping. This protocol is secure because the key itself does not contain any information that needs to be kept private and if the key is known to be compromised, it is not used to encode any private data. The major achievement of quantum cryptography is to change the foundation of security from computational assumptions (the difficulty of solving hard mathematical problems) to assumptions based only on the laws of physics.

For those with some prior knowledge of quantum mechanics, a more detailed example of quantum key distribution is presented. There are many protocols and realizations; this example will use the polarization state of photons to encode the qubits of information and pairs of entangled photons. The underlying principle of this protocol is to use the quantum mechanical property that measuring a state that is not an eigenstate of the measurement operator will result in a random outcome which can be detected. Assuming that the polarization of two photons can be prepared in the state $(|H_A, H_B\rangle - |V_A, V_B\rangle)/\sqrt{2}$ where H_i and V_i represent horizontal and vertical polarizations respectively for photons at two parties Alice (A) and Bob (B). It turns out that this state can be rewritten in the basis where $|\pm 45_i\rangle = (|H_i\rangle \pm |V_i\rangle)/\sqrt{2}$ as $(|+45_A, +45_B\rangle - |-45_A, -45_B\rangle)/\sqrt{2}$. If Alice and Bob measure in the $\{H, V\}$ basis, they will randomly see the result horizontal (H) or vertical (V). However, there will be a 100% correlation between their respective measurements. In other words, when Alice measures H then Bob will also measure H and likewise for V. If Alice and Bob both measure in the $\{+45$ or $-45\}$ basis, their results will also have a 100% correlation agreement (recall also that if we measure the state H in the $\{+45$ or $-45\}$ basis, the result is randomly $+45$ or -45 .) On the other hand, if the two parties measure in different bases, there will be no correlation in the measurement results. With this in mind, the following is the protocol for establishing a key:

1. Alice and Bob independently construct their own string of random bits 0 and 1, such as $B_a = 0_1 1_2 0_3 0_4 \dots$ and $B_b = 0_1 0_2 1_3 0_4 \dots$ where the subscript refers to the pair of photons.
2. Individual pairs of photons are sent to Alice and Bob, and each party measures the polarization of the photon in a basis which is decided from the random strings B_i . If the i th string element, B_{ip} , is 0, the $\{H, V\}$ basis is chosen. $\{+45, -45\}$ is chosen if the i th element is 1.
3. The parties exchange the strings B_a and B_b , then discard results of polarization measurements where their string elements happen to be different. Without an eavesdropper present the remaining results of measurement should be identical since they have been measured in the same basis. The results themselves are random in the sense that they would be measured randomly as H or V, for example, however, Alice and Bob do always have the same result, whatever it may be. If one measured H, the other will have measured H as well, and similarly for V.

4. The two parties now check if an eavesdropper, called Eve, was present. For Eve to determine what is being transmitted, she must choose a basis and make a measurement. For half of her choices, the measurement will occur in the same basis as Alice and Bob, and for the other half, her measurement will occur in a different basis. In that latter case, her measurement will destroy the entangled state, reducing the correlation of measurement results between Alice and Bob. This reduced correlation can be detected by sampling some of the results of the measurements and exchanging them publicly. If no reduction in correlation is detected, Alice and Bob can safely use the remaining measurement results as a key to encrypt information. If an eavesdropper is detected, the parties drop the string of measurements, and start again.

Note that Alice and Bob must keep each basis they use a secret until the measurements are made. Otherwise, the eavesdropper would know which basis to measure with to avoid causing errors. Another important point is that the key itself does not contain any private information, it is simply a means to make some desired information secret after it is established.

It turns out that building quantum cryptography prototypes is more straightforward than building prototypes of quantum computer. At Waterloo, we have today a quantum cryptography prototype using entangled photons. A source of photon pairs is located on the roof of the CEIT building at UW, which uses telescopes to send one to the IQC and the other to the Perimeter Institute. We then implement the quantum cryptography protocol and exchange information securely.

Quantum cryptography can be described as is the lowest hanging fruit in the panoply of quantum technologies. There are about a hundred groups in the world who are working on quantum cryptography, everywhere from North America and Europe to South Africa. Already today, there are several companies around the world starting to market quantum cryptography products. It is promising that, today, we are able to control one part of the quantum world. An overview of the state of quantum cryptography can be found in www.iqc.ca/+laflamme/reports/QKD-CSERCreport080416.pdf

Canada, is a world-wide leader in quantum information science and in particular quantum cryptography, in fact the concept was co-invented by Gilles Brassard at the Université de Montréal in 1982. We have at present two national networks of scientists that work in this area: CIFAR (Canadian Institute for Advanced Research, www.cifar.ca) which focuses on fundamental aspect of quantum information science; and QuantumWorks (www.quantumworks.ca), with headquarters in Waterloo, is an Innovation platform from NSERC that aims to bring together academia, government and industry and to investigate the various elements of quantum cryptography technology. There is also the Institute for Quantum Computing at the University of Waterloo (www.iqc.ca) that brings together about 100 researchers and has a strong international reputation.

In conclusion, humans are curious and this leads us to observe the world around and try to understand it. Understanding and controlling aspects of our world has, and can dramatically change our way of life. Quantum properties of nature have the potential to create a technological revolution. Because of Moore's law it seems inevitable that we will encounter them, and possibly take advantage of them by producing new technology with incredible power. In the last 10 years, we have learned how to theoretically control quantum systems, and experiments are well under way demonstrating the basic principles. The next years will be very exciting. Not only may quantum mechanics produce fundamentally different technolo-

gies than what we have already seen, but also give a very different perception of the world than the one inherited by classical theories of the 17th, 18th and 19th centuries. We are discovering a new world, crossing a new ocean to unexplored territories, and I wonder what will people think of our adventure 400 years from now.

ACKNOWLEDGEMENTS

We would like to thank the government of Ontario, CIFAR and NSERC for support.