Dr. Michele Mosca, co-founder and deputy director of the Institute of Quantum Computing at the University of Waterloo, holding a D.Phil in Quantum Computing Algorithms, and specializing in the same as well, gave a talk on Quantum Computing on the 14th of March. Dr. Mosca started off his talk by explaining how modern physics came to be, and how one of its consequences is the field of quantum computing.

The paradigm shift was initiated when the results of experiments couldn’t be explained by theories and a physical model set up at that time. Some of these phenomenon included Photoelectric Effect, Discrete Spectrum of Atomic Radiation, Stability of atoms, Polarization of light etc. The onset of the Quantum Theory explained several of these phenomenon. But it also brought along with it much more.

It was much unlike classical physics and failed intuition to a great extent. Dr. Mosca demonstrated this with a fairly simple example of Quantum Interference. A compounded beam splitter, which would normally be expected to give a 50% reading on both the receivers, in fact, gives a 100% reading in one. This result can’t be obtained by a normal probabilistic treatment. The concept of probability amplitudes, which can have complex phase factors (negative probability) needs to be applied.

The Quantum Paradigm had implications that made people, including its founders, uncomfortable. However, it is now the dominant paradigm for physics. Alan Aspect, provided the first experimental verification of the Quantum Theory which contradicted the classical “local hidden variables” theories.

A Quantum Computer is similar to an ordinary one, with the difference being in the implementation of a bit. A Quantum bit (or Qubit) exists as a Linear Combination of All possible states of that bit. Therefore, for simulating n Qubits, one needs to keep track of 2n quantum amplitudes. Qubits are currently being experimented on by trapping ions (also, another technique using Rydberg atoms) which seems to be the path forward. Performance of Superconducting Circuits has shown significant improvement over the years.

Quantum Computers could potentially be used to simulate quantum mechanical systems, counting and optimization, previously intractable mathematical problems (some cases underlying modern cryptography) etc. Peter Shor showed that main key establishment protocols would be broken down by a quantum computer. This calls for a new “quantum-safe” cryptographic infrastructure. This type of cryptography can achieve security on the cloud as well. Dr. Mosca believes that the current infrastructure is susceptible and that the need for this solution is imminent.

He elaborated on the 7 fundamental stages of Quantum Information Processing. Developing logical Qubits with longer lifetime than physical Qubits is where current research is focused on. He also, approximates that a fault-tolerant system will developed within the next five years, after which, building a useful and reliable quantum computer will be within our reach.

There are other sides to the larger solution as well, can the new quantum-safe cryptographic solution be integrated with the existing infrastructure? Are the current standards, practices and computational paradigms feasible for a new quantum one? These are the questions that will be answered as the future unfolds. A Quantum Computer may still be a long way down the road, but the destination is not unclear as it was a few years ago.