Quantum Computing and Quantum Communication

"Because it's there!" –

George Mallory,
(before dying on Mt. Everest, on why he wanted to climb it)

Why build a quantum computer? Because it's not there, for one thing, and the theory of quantum computation, which far outstrips the degree of implementation, suggests that a quantum computer would be an incredible machine to have around. It could factor numbers exponentially faster than any known algorithm, and it could extract information from unordered databases in square root the number of instructions required of a classical computer. A quantum computer would also have profound applications for pure physics. By their very nature, quantum computers would take exponentially less space and time than classical computers to simulate real quantum systems, and proposals have been made for efficiently simulating many-body systems using a quantum computer.

In a quantum computer, the fundamental unit of information is called a quantum bit or qubit. Qubits are represented by systems that have two clearly distinguishable states, $|0\rangle$ and $|1\rangle$ Qubits possess the unique quantum mechanical property known as superposition, i.e., a qubit can simultaneously be in both the one and zero states with a complex coefficient representing the amplitude for each state. The real power of quantum computation derives from the exponential state spaces of multiple quantum bits: just as a single qubit can be in a superposition of 0 and 1, a register of n qubits can be in a superposition of all 2n possible values. These states that lead to the exponential size of the quantum state space are called the entangled states. In a traditional computer, information is encoded in a series of bits, and these bits are manipulated via Boolean logic gates arranged in succession to produce a result. Similarly, 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. On applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits that are in some initial input state. The qubits can then be measured, with this measurement serving as the final computational result.

The talk will cover the basics of quantum computing from phenomena like quantum superposition and quantum entanglement and will extend to quantum communications. A brief review of quantum communication protocols and latest technological attempts to realise the technology will also be covered.