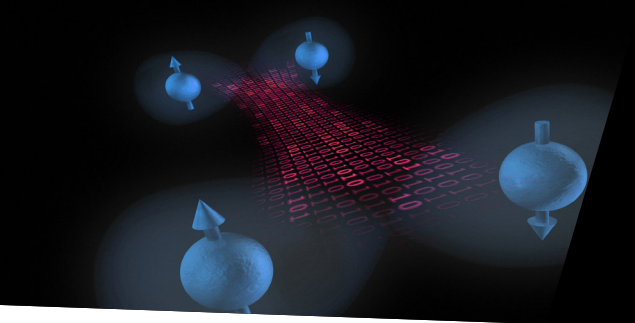

QUANTUM INFORMATION

DISCOVERY

Quantum physics describes the behaviour of the unbelievably tiny: electrons, nuclei, atoms, molecules, and other particles. The laws that govern the behaviour of these particles are very different than those of the everyday world. For example, quantum particles can be in a *superposition* of seemingly contradictory states at the same time – not just here or there, but here *and* there!

In the 1980s, scientists proposed that, if these unique quantum phenomena could be properly harnessed and controlled, they could be used to store, process, and protect information in powerful new ways. Thus began the age of quantum information research.

INNOVATION

Quantum computing is expected to revolutionize how we use, process, and share information. Your computer today uses bits – ones and zeros – to solve mathematical problems and manipulate information. But there are some computational problems that are too taxing for "classical" computers to ever efficiently tackle. A quantum computer, however, exploits the superposition principle to process information in a radically new way that, for certain computational tasks, leads to tremendous – even exponential – gains in speed and efficiency. Although still in prototype stages, quantum computers have vast potential. They will be paramount to designing new materials and medicines, gaining a deeper understanding of our universe, and much more.

Quantum cryptography – the use of quantum technology for ultra-secure communications – is another important facet of quantum information and is already being deployed in the marketplace. Because quantum particles are so tiny and sensitive to disturbance, even observing them will measurably alter them (this is known as Heisenberg's uncertainty principle). Any eavesdropping on a communication encrypted with quantum information is, therefore, immediately detectable.

In conventional cryptography, information is encoded using a "secret key" – and only the parties who have that key can decode the message. In today's cryptography, that key is typically created using very hard-to-solve mathematical problems. But this technique, although safe today, may be jeopardized by breakthroughs in computing (including quantum computing). Thankfully, Heisenberg's uncertainty principle can be exploited to remove this "computational" weakness variable. Generating a key using the states of quantum particles means that any attempt by an eavesdropper to snoop will be detectable. This allows the parties communicating to be certain of when they're free from eavesdropping, letting them set up a key that's guaranteed to be secure.

Quantum cryptography is so secure that banks and governments are already using it, and it has even been used to protect the secrecy of ballots in a Swiss election.

Research in quantum information has also led to the development of ultra-precise, selective, and efficient quantum sensors. These sensors utilize a range of quantum properties such as superposition, entanglement, and quantum feedback to probe the nanoscale world. Such precise sensors could have applications including geological exploration, molecular imaging, medical diagnosis, and beyond.

IMAGINATION

We are only beginning to imagine the incredible possibilities of quantum information technologies. Noted physicist Paul Davies wrote: "The 19th century was known as the machine age; the 20th century will go down in history as the information age; I believe the 21st century will be the quantum age."

What problems do you think ultra-powerful quantum computers will help solve? How would you use quantum-encrypted secret codes?