ROSEDALE ACADEMY

Physics Journal Group Activity

Working in groups of 2-3, read the following article. Afterwards, work together to answer the questions provided. For question 7, get together with another group and discuss your findings with one another.

Raymond Laflamme and Quantum Information Theory

Abstract

Raymond Laflamme is a leading thinker in the world of quantum mechanics, quantum computers, and the nature of our universe. He is a faculty member of the Perimeter Institute for Theoretical Physics in Waterloo, Ontario. Laflamme is enthusiastic about the current quantum research and the promises it holds for the future.

Introduction

Raymond Laflamme (**Figure 1**) grew up in Quebec city, where he studied physics at University Laval. He then worked as a doctoral student with Stephen Hawking, a world-renowned theoretic physicist best known for his work in cosmology and quantum gravity, at the University of Cambridge. While working there, Laflamme convinced Hawking that, in a contracting universe, time does not reverse. That story is retold in Hawking's book *A Brief History of Time*. In 2001, after working as a researcher at different laboratories around the world, Laflamme joined the Perimeter Institute for Theoretical Physics in Waterloo, Ontario. He is also director of the Institute for Quantum Computing at the University of Waterloo.

Figure 1 Laflamme is a Canadian pioneer in the study of quantum computing, specializing in error-correcting codes.

Quantum Information

As a research scientist at Los Alamos Research Laboratory, New Mexico, from 1992 to 2001, Laflamme became interested in quantum computing. Traditional computers operate

through the manipulation of bits of data that list in one of two stats: 0s and 1s. Quantum computers, by contrast, are not limited to these two states. Instead, they encode data as quantum bits, or qubits, which can exist simultaneously as either a 0 or a 1 or as a superposition of the two. Physical qubits can be constructed from atoms, ions, photons, or electrons that work together as the computer memory and processor. A quantum computer can store and process information in multiple states simultaneously, so its computing power has the potential to surpass even the most powerful of traditional computers.

Quantum computing can open up a whole new domain for computers that may allow even persona computers to perform tasks never before dreamed of. A quantum computer, for example, can search elections of information, or databases, much more quickly than a classical computer. This ability would allow an increase n the speed of websites that use databases, including web browsers and social networking sites. A quantum computer can also encode information and decode encrypted information much more quickly than a classical computer.

Quantum information theory is Laflamme's passion. This field of study proposes that physical information about a system can be stored in a quantum state. This storage allows levels of information processing and encrypting that are not possible in the classical world. Quantum information theory leads to the type of quantum information processing that makes transmitting information completely secure.

At the Perimeter Institute, Laflamme collaborated in devising a mathematical framework for error-correcting codes in quantum computing. When information is stored or transmitted from one computer to another, errors in the information can arise due to accident, noise, and other problems. Error-correcting codes detect and correct these errors, so error correction is an important part of designing a reliable computer.

Quantum error correction prevents errors in quantum computers. Errors can arise from noise in the circuits and from interference from outside the computer. Noise comes from unwanted, meaningless data, often as an unwanted by-product of other transmissions. Quantum information can also be affected by a quantum effect called decoherence, which causes a quantum system to behave more like a classical system. Decoherence is a sort of "quantum noise" that reduces the quantum computer's advantage over current computers. Laflamme is working to develop methods for protecting quantum information against such noise. As of 2011, Laflamme's research group's 12-bit quantum computer is the world's largest quantum processor.

Development in Quantum Cryptography

Cryptography is the science of encoding and decoding information in order to store and transmit it securely. Whenever you log in to a website, for instance, your login information will pass from your computer over the Internet in an encoded form to prevent anyone from stealing your information. Researchers see cryptography as an important application of quantum information science that will allow us dos end information through public systems such as fibre optic networks without fear that the information could be intercepted.

Traditional cryptographic methods of encoding and decoding messages use mathematical codes and keys. For example, encryption software on a computer generate a key, which determines a random code and encrypts an email message with the code before sending it over the Internet. When the message is received, the key deciphers the message. Keys are very large numbers. The larger the key, the more number combinations are possible, making it more difficult to break the code. With standard encoding methods, it is impossible to know with certainty whether the key has been intercepted by an eavesdropped.

Quantum cryptography uses quantum mechanics. Recall from Section 10.5 that electromagnetic waves can be polarized. In the same way that electromagnetic waves can be polarized, so too can photons. Users of quantum cryptography will first exchange a key, which is a code connected to the polarization of the photons. Basically, the photons carrying the message are polarized in a certain direction, and the receiver must know the direction. The sender uses the key to lock the information, and the receiver uses the key to unlock the information.

An eavesdropped must know the direction of polarization to intercept the message. Measurement of a single photon's polarization, though, affects the polarization differently than the measurement of a classical wave, predicted by the Heisenberg uncertainty principle. So, unlike traditional cryptography methods, with quantum cryptography it is possible to detect whether or not the key has been intercepted. An eavesdropper will always be detected because it is impossible to measure (eavesdrop on) a quantum system without fundamentally changing it. Banks in Switzerland are already using quantum crytography to encode information. Figure 2 hows an example of some quantum cryptography equipment.

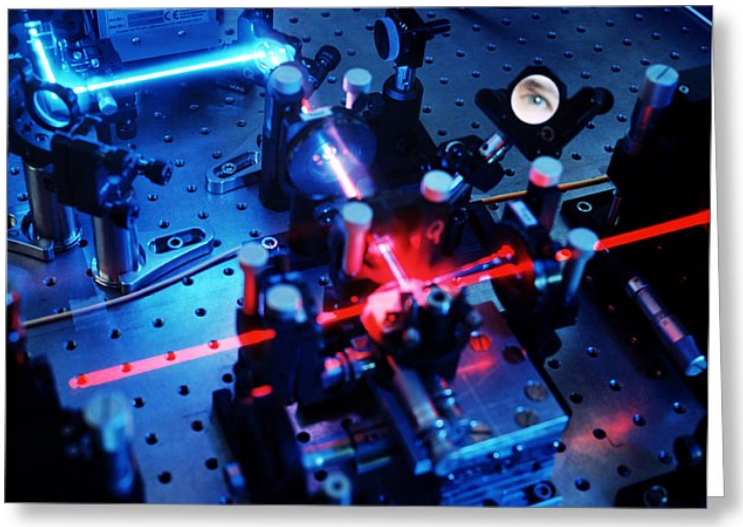

Figure 2 Quantum cryptography equipment uses lasers to produce streams of photons with particular polarizations.

Questions

1. Explain some of Laflamme's contributions to quantum research.
2. Describe the significance of Laflamme's work in developing quantum error-correcting codes.
3. Describe the relationship between quantum information theory and its application in quantum cryptography.
4. How do decoherence and noise affect information transmission?
5. Describe the impact of Laflamme's research on society. What impacts could this have on you personally?
6. How do quantum computers differ from traditional computers?
7. Research Laflamme and his current projects and areas of expertise. Discuss and describe one of the research projects with another group.

Adapted from Nelson University Preparation - Physics 12.