Applying Quantum Technologies to Computer Science

As a computer engineering undergraduate at Texas A&M University, **Mark M. Wilde** first read about quantum computers and was blown away by the idea of computers capable of so much more than computers of that time. His life goal became to learn quantum mechanics – the principles on which quantum computers would work. After some years, he began making fundamental contributions that have had a lasting impact on the fields of quantum computation and communication.

Wilde's work eventually led him to the Department of Physics & Astronomy at Louisiana State University, where he is an assistant professor and holds a joint appointment with the Center for Computation & Technology (CCT). Currently, Wilde is working to develop algorithms for quantum information processing that could help make quantum computation and communication a reality.

"One major question that drives my research is to find out what are the fundamental limits of communication," Wilde said. "In order to do so, you need to bring the laws of quantum mechanics into the picture. My work is interdisciplinary. The field of quantum communication draws on physics, mathematics, computer science, and electrical engineering."

The basic building block of a quantum computer is a qubit, just as the bit is for an ordinary computer. A qubit is the smallest quantum system imaginable, and like a computer bit, it has two states: on and off. But, in some sense, qubits can be both on and off at the same time. Along with an odd phenomenon called entanglement, in which quantum particles are very strongly correlated, these simultaneously on-and-off states are responsible for the much faster speeds expected with quantum computing.

"It's also hard to simulate quantum systems with ordinary computers," Wilde said. "For example, there are so many different states of 500 qubits that describing the evolution of them according to quantum mechanics would require a 2^{500} by 2^{500} matrix of numbers. That's hard to do on an ordinary computer."

Building a quantum computer is a very complex challenge, since individual atoms, electrons, or photons must be addressed and managed. In the operation of a quantum computer, a lot of errors can arise when processing finely tuned qubits due to their interaction with the surrounding environment, causing the qubits to lose information. However, quantum error correction algorithms have been devised to avoid the deleterious effects of these environmental interactions, and "they can be simulated using the supercomputing resources at CCT," Wilde said.

A quantum computer, once developed, would be able to crack the encryption codes we use today. This is one major application of quantum computers that has interested corporations such as IBM, Google, and Lockheed Martin, among others, in addition to various governments around the world.

On the other hand, "what quantum takes away it also gives back," Wilde said. "Quantum key distribution would provide stronger security than any current cryptosystem in use because if someone tampers in any way with the transmission of quantum information it could be detected. This is a consequence of the uncertainty principle, a cornerstone of modern physics, and quantum key distribution algorithms are based on this principle."

In a recent *Nature Communications* journal article, Wilde and his coauthors published their findings on quantum secured communication protocols. In particular, their work discusses the limits on secret data exchange over long distances. He and his coauthors proved mathematically that the rate at which information can be communicated securely, even using the laws of quantum mechanics, decays exponentially with the distance over which the data is communicated. More simply, the greater the distance between two quantum computers communicating, the less chance there is that these two quantum computers can communicate securely. However, this loss can be mitigated through the use of a device called a "quantum repeater."

Wilde collaborated on this project with a researcher in Tokyo and a colleague at Raytheon BBN Technologies in Cambridge, Maine. He also has active collaborations with various research groups around the world. Along with **Jonathan P. Dowling** and **Hwang Lee** of the Quantum Science & Technologies Group, Wilde jointly supervises Ph.D. student **Bhaskar Roy Bardhan** who will soon graduate and start a postdoctoral position at MIT.