More accurate than Heisenberg allows? Uncertainty in the presence of a quantum memory

July 27 2010

Quantum cryptography is the safest way to encrypt data. It utilizes the fact that transmitted information can only be measured with a strictly limited degree of precision. Scientists at Ludwig-Maximilians-University in Munich and ETH Zurich have now discovered how the use of a quantum memory affects this uncertainty.

A quantum particle is hard to grasp, because one cannot determine all its properties precisely at the same time. Measurements of certain parameter pairs such as position and momentum remain inaccurate to a degree given by Heisenberg's Uncertainty Principle. This is important for the security of quantum cryptography, where information is transmitted in the form of quantum states such as the polarization of particles of light.

A group of scientists from LMU and the ETH in Zurich, including Professor Matthias Christandl, has now shown that position and momentum can be predicted more precisely than Heisenberg's Uncertainty Principle would lead one to expect, if the recipient makes use of a quantum memory that employs ions or atoms. The results show that the magnitude of the uncertainty depends on the degree of correlation ("entanglement") between the quantum memory and the quantum particle. "The result not only enhances our understanding of quantum memories, it also provides us with a method for determining the degree of correlation between two quantum particles", says

Christandl. "Moreover, the effect we have observed could yield a means of testing the security of quantum cryptographic systems." (Nature Physics online, July 25, 2010)

Unlike classical computers, quantum computers operate not with bits, but with quantum bits or qubits, quantum mechanical states of particles. The crucial feature of qubits is that they can exist in different states at once, not just 0 or 1, but also as a superposition of 0 and 1. The ability to exploit superposition states is what makes quantum computers potentially so powerful. "The goal of our research is to work out how quantum memories, i.e. memory systems for qubits, might be utilized in the future and how they affect the transmission of quantum bits", explains Christandl, who left LMU Munich in June 2010 to take up a position in the Institute of Theoretical Physics at the ETH in Zurich.

Heisenberg's Uncertainty Principle plays a central role in quantum computing, because it sets a fundamental limit to the accuracy with which a quantum state can be determined. Quantum mechanics also tells us that the measurement of a parameter can itself perturb the state of a particle. If, for example, one were to measure the position of a particle with infinite precision, the particle's momentum would become completely uncertain. Quantum cryptography uses this effect to encrypt data, for instance by entangling two quantum particles in a way that the probability with which the measurement of one particle yields a certain value depends on the state of the other particle. Eavesdropping can thus easily be uncovered, because any measurement will change the state of the particle measured.

The teams at LMU and the ETH Zurich have now shown that the result of a measurement on a quantum particle can be predicted with greater accuracy if information about the particle is available in a quantum memory. Atoms or ions can form the basis for such a quantum memory. The researchers have, for the first time, derived a formula for

Heisenberg's Principle, which takes account of the effect of a quantum memory. In the case of so-called entangled particles, whose states are very highly correlated (i.e. to a degree that is greater than that allowed by the laws of classical physics), the uncertainty can disappear. According to Christandl, this can be roughly understood as follows "One might say that the disorder or uncertainty in the state of a particle depends on the information stored in the quantum memory. Imagine having a pile of papers on a table. Often these will appear to be completely disordered -- except to the person who put them there in the first place."

"Our results not only improve our understanding of quantum memories, they also give us a way of measuring entanglement", says Christandl. "The effect could also help us to test the security of quantum cryptographic systems." One can picture the method as a game in which player B transmits a particle to player A. A then performs a measurement on the particle, introducing an uncertainty. A subsequent measurement by B will only yield the value determined by A with an uncertainty given by Heisenberg's Principle. "But if B uses a quantum memory", says Christandl, "he can determine the correct value and win the game."

More information: "The Uncertainty Principle in the Presence of Quantum Memory", M. Berta, M. Christandl, R. Colbeck, J.M. Renes, R. Renner
Nature Physics, 25 July 2010. DOI:10.1038/nphys1734

Provided by ETH Zurich