Maximizing Confidence in Quantum Information Decoding

November 21 2006

When it comes to quantum information processing and cryptography, retrieving information encoded in orthogonal quantum states can, in principle, be done perfectly (although in practice it may be hard to implement). When it comes to non-orthogonal quantum states, however, the necessary discrimination between states in order to extract information becomes a daunting task.

Sarah Croke of the Universities of Strathclyde and Glasgow in Scotland explains how non-orthogonal states are different:

“It is not that the measurement is difficult experimentally, rather that perfect discrimination is actually forbidden by the laws of physics. Since people started thinking about using quantum states to store and manipulate information, it has become important to know how to optimally discriminate between different quantum states because at some point it will be necessary to retrieve the information encoded in a quantum system, and to do this it is necessary to try to measure its state.”

Croke points out that in non-orthogonal quantum states, some error will always be involved. The idea, she says, is to minimize the probability that the wrong state will be chosen, thus improving the probability that the state carrying the intended quantum information will be chosen. “We have designed a network such that the probabilities for what we want from these more complicated measurements are higher,” Croke tells *PhysOrg.com* via telephone. “For this network *when* the result of measurement leads us to identify a certain state, the probability that the

system really was in that state is maximized."

Croke and her co-authors, Peter Mosley and Ian Walmsley at the University of Oxford and Stephen Barnett at the University of Strathclyde, are the first to experimentally realize an explicit improvement in the confidence of quantum state discrimination in linearly dependent states over the optimal minimum error measurement. Indeed, until the results of this experiment, which are published in *Physical Review Letters* in an article titled, "Experimental Realization of Maximum Confidence Quantum State Discrimination for the Extraction of Quantum Information", the possibility of such confidence for linearly dependent states was in question, although it had been demonstrated for linearly independent states.

"In our experiment," Croke explains, "we use three states. It is the simplest example of a linearly dependent set, and the measurement has four possible outcomes. We show how to maximize the probability that you will get the correct answer — that you can have greater confidence that the state you have found is, in fact, the state containing the information sent to you." Croke says that the fourth result in the experiment is inconclusive, providing no information at all. However, she insists, "If any of the other three results are obtained, we can be as confident as possible that the state indicated really was the state that entered the optical network."

As Croke explains it, quantum information sent over secure channels, mainly for cryptography purposes, is sent in a specific state. She provides a scenario, via email, in which a sender (referred to in quantum cryptography as Alice) encodes information for a recipient (denoted as Bob):

"Alice and Bob have pre-agreed what states could be sent, and what information each of these represents. Thus Alice encodes a message by

preparing a quantum system in one of the pre-agreed states. When Bob receives the system, his job is to determine which quantum state the system is in, in order to decode the information sent by Alice. When the state arrives Bob doesn't know what that state is, and thus needs to make a measurement to try to find out which state he has received."

Non-orthogonal quantum states are preferred for cryptography because eavesdroppers have no way to perfectly decode the message. Additionally, it is possible to detect possible eavesdroppers because quantum systems are disturbed by any attempt at measurement. So, in principle, not only would a third party be unable to decode the message at all, but such an intruder would be detected by Alice and Bob. "[I]t is not so much that quantum information is sent over secure channels in quantum cryptography, rather that the channel is secure *because* it is a quantum channel," Croke writes in an email.

Croke and her colleagues have demonstrated a method that can be used when confidence in the result is more important than whether or not a result is obtained. "With other methods," says Croke, "you always get a result. But it could be the wrong result. Our experiment shows a way that you may not always get a result. But when you do get a result, you can have the greatest confidence possible that it is the correct result." With the Oxford-based experiment, that confidence is expressed as a 2/3 probability.

The team from the U.K. used optical polarization in their experiment, as a two-level system with linear optical elements used to create and then manipulate the quantum states. Their implementation shows that optimal maximum confidence can be achieved when attempting to identify any given state in a set of quantum states. And, while this information is obviously important in terms of cryptography, Croke also points out that it is important for quantum information processing. "After all," she insists, "You need to make some sort of measurement, and you need to

be able to extract the information received from the computation."

But, while Croke thinks that the method described in this paper could be useful to quantum information processing, she admits that she isn't sure how practicable it would be. "We're not sure exactly how it would work," she says. "There are several architectures under development for use in quantum information processing. One such architecture is linear optics, using photons as information carriers. The type of measurement described in our paper could easily be applied to these systems."

Croke continues: "For other architectures such as ion trap, cold atom, NMR, linear optics using coherent states, it may not be as easy to implement this sort of measurement. We have been talking to people working in quantum computing to find out what sort of states they may be interested in discriminating between, and we are thinking about whether it is possible to implement the optimal maximum confidence strategy for these systems.

By Miranda Marquit, Copyright 2006 PhysOrg.com