

Classical communication problem solved using quantum entanglement

One of the problems plaguing classical communication is associated with what is known as the Byzantine agreement. In this problem, messages between three different parties are subject to faulty information. Quantum communication, though, has held the promise of solving this dilemma. But until now, it has been difficult to do so, even using entangled states.

However, an international group of scientists may have found a solution. The results of their experiment are published in *Physical Review Letters*: “Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection.”

“Instead of only three photons,” Harald Weinfurter tells *PhysOrg.com*, “our protocol uses four photons in a specially prepared state.” Weinfurter is associated with the Max Planck Institute for Quantum Physics in Garching, Germany, and with the Ludwig Maximilians University in München. Weinfurter worked with Sascha Gaertner, a colleague at Max Planck and Ludwig Maximilians, who did a great deal of the experimental work. Also included in the effort were Mohamed Bourennane at Stockholm University, Christian Kurtsiefer at the National University of Singapore and Adán Cabello at the University of Seville in Spain, who “came up with most of the idea,” Weinfurter says.

“Our protocol allows us to find the liar between three partners sending messages,” Weinfurter continues. “It offers a verifying process that two receiving computers will cross check with each other. It is a way of solving this Byzantine agreement problem.”

The problem, explains Weinfurter, comes from a story Lamport, et al. described in 1982, creating a situation that might have taken place in 1453 when Constantinople was besieged. Generals were sending messages back and forth, trying to coordinate an attack on the city. Some, for their own reasons, attempted to use false information to sabotage the others.

In quantum mechanics, the problem of three-party communication also includes faulty information as messages are passed and forth. It can be difficult – almost impossible until now – to detect the faulty information and its source in a three-party quantum communication setup. This is because the required qutrits, threefold valued quantum systems, are quite difficult to generate and handle.

Experimentally, it is much easier to create qubit (two-party) entangled states. Weinfurter and peers succeeded in overcoming the qutrit difficulties by setting up a system that creates four-qubit entangled states. “We use a pulsed laser, and even though you usually only get two photons, there is a reasonable possibility for four photons,” he says. “Once these are detected, they can be entangled. The state comes out of the source, more or less.”

Weinfurter says that this protocol is not actually for secure communication, only. “It’s really for verification,” he explains, “so you can detect the liar.” The special state of the entangled photons is used to distribute the key used in the verification process.

Unfortunately, Weinfurter admits, the setup is difficult to use in a computer. “For use in data replication, more developments are still required.”

The important thing, he insists, is that this experiment shows, for the first time experimentally, a way to defeat the Byzantine agreement problem. “For a practical quantum computing application it’s not there,”

Weinfurter says. “But with new methods to create photons, we could get there soon.”

Copyright 2007 PhysOrg.com.

All rights reserved. This material may not be published, broadcast, rewritten or redistributed in whole or part without the express written permission of PhysOrg.com.

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.