MAX PLANCK INSTITUTE
OF QUANTUM OPTICS

Garching, 22.02.2008

Press Release

Liars, be careful!

Novel quantum protocol developed by MPQ-LMU scientists solves „Byzantine Agreement"

Press & Public Relations,
Dr. Olivia Meyer-Streng

Phone:
+49(0)8932 905-213
E-mail: olivia.meyer-streng@mpq.mpg.de

Imagine two of your friends tell you – independently - about an agreement for a next meeting. Each of them however mentions a different meeting point. How do you find out who is the liar? And how can you finally succeed to meet at least the honest one at the right time and place? A new quantum protocol, devised by an international team of scientists around Prof. Harald Weinfurter (Max Planck Institute of Quantum Optics, Garching, and Ludwig Maximilian's University Munich) can now help you with the decision (Phys. Rev. Lett., 100, 070504 (2008)). In classical communication theory problems of this kind are named "Byzantine Agreement". They frequently occur e.g. in the communication between computers, in fault tolerant computing, or in database replication.

The problem of detecting the fault or the liar in a communicating system of exactly three parties A, B, and C, is only solvable if each of the partners is in possession of a code, a list of numbers that are strongly correlated with each other. But how can we generate such lists, and how can we ensure them not to be manipulated? The answer to this is given by quantum theory: strongly correlated lists can be produced with the help of entangled quantum particles.

Quantum communication between two partners by two entangled twin photons is more or less state of the art by now. Communication between three partners requires new methods. The best way would be to use triple-states of so called qutrits, quantum particles that can be in three different states. It is however difficult to realize qutrits experimentally. The concept of the Munich group, suggested by the theoretician Adán Cabello of the University of Sevilla, instead uses four entangled qubits. Two are sent to partner A, each one to B and C.

The team of Prof. Harald Weinfurter has now succeeded to implement this kind of quantum protocol experimentally at Max Planck Institute of Quantum Optics. The physical qubits are polarized photons, and the states 0 and 1 correspond, respectively, to the vertical and horizontal polarization states. The required system of four entangled photons is generated by means of a non linear crystal and bright laser pulses. The photons get distributed, and their polarisation is determined by each partner independently. Since all of the photons are entangled the results

Hans-Kopfermann-Str. 1
D-85748 Garching

Phone:+49(0)8932 905-0
Fax:+49(0)8932 905-200

of the measurements are strongly correlated. By comparison of some test bits the partners are able to prove the security of the distribution (similar to quantum cryptography) and obtain a list that is perfectly suited for the detection of liars. [O.M.]

Original publication:
Sascha Gärtner, Mohamed Bourenanne, Christian Kurtsiefer, Adán Cabello, and Harald Weinfurter
“Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection “
Phys. Rev. Lett., 100, 070504 (2008)

Contact:

Prof. Harald Weinfurter
Department of Physics
Ludwig-Maximilians-Universität München
Schellingstraße 4
80799 München
Phone: +49 - 89 / 2180 2044
e-mail: harald.weinfurter@physik.uni-muenchen.de

Dr. Olivia Meyer-Streng
Press & Public Relations
Max Planck Institute of Quantum Optics
Phone: +49 - 89 / 32905 213
Fax: +49 - 89 / 32905 200
e-mail: olivia.meyer-streng@mpq.mpg.de