Q 33 Quantenkommunikation II

Zeit: Dienstag 10:45–12:00 Raum: HU Audimax

Q 33.1 Di 10:45 HU Audimax

Angular EPR paradox — •Jörg B Götte, Sonja Franke-Arnold, and Stephen M Barnett — University of Strathclyde, Department of Physics, 107 Rottenrow, G4 0NG Glasgow, United Kingdom

Orbital angular momentum [OAM] of light provides a multidimensional optical system suitable for quantum communication. Entanglement is the basis of most applications in the field of quantum information. In this context it would be desirable to demonstrate the EPR paradox for the conjugate variables of OAM and azimuthal position. We discuss quantum correlations in these variables for photon pairs created in a parametric down conversion. Modelling the measurement of OAM and azimuthal position of photons on previous experimental work in this field, we are able to propose an experimentally feasible criterion for the demonstration of an angular EPR paradox, which includes a description for the indeterminacies inherent to the measurement process. We discuss the effects of these uncertainties to the proposed criterion.

Q 33.2 Di 11:00 HU Audimax

Discrimination of two mixed quantum states — •Ulrike Herzog[1], János A. Bergou[2], and Oliver Benson[1] — [1]Institut für Physik, Humboldt-Universität zu Berlin — [2]Department of Physics, Hunter College, City University of New York

Distinguishing nonorthogonal quantum states is a basic prerequisite in quantum communication. Different measurement schemes have been developed to accomplish this task in an optimized way. Minimum-error discrimination yields an ambiguous result, with a minimum probability that it is erroneous. Optimum unambiguous, i. e., error-free, discrimination is a probabilistic measurement with a minimized probability of getting an inconclusive outcome, where the measurement fails to give a definite answer.

We consider the discrimination between two arbitrary but known mixed quantum states, occurring with given prior probabilities. In this case the lower bound of the failure probability in unambiguous discrimination is proportional to the fidelity of the two states [1]. Making use of an alternative derivation of the lower bound, we discuss the conditions under which it can be actually reached in a generalized measurement. For special given states we determine the detection operators describing the measurement that yields optimum unambiguous discrimination. We also show that the minimum failure probability in the error-free measurement scheme is always at least twice as large as the minimum error probability in ambiguous discrimination [2].

[1] T. Rudolph *et al.*, Phys. Rev. A **68**, 010301(R) (2003).
[2] U. Herzog and J. A. Bergou, Phys. Rev. A **70**, 022302 (2004).

Q 33.3 Di 11:15 HU Audimax

Detecting quantum correlations in quantum key distribution protocols — •O. Gühne[1], M. Curty[2], M. Lewenstein[3], and N. Lütkenhaus[2] — [1]Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, A-6020 Innsbruck — [2]Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, D-91058 Erlangen — [3]Institut für Theoretische Physik, Universität Hannover, Appelstr. 2, D-30167 Hannover

Quantum key distribution (QKD) enables secure communication between two parties. For practical implementations it is important to know under which conditions a given QKD protocol is secure or not. It has been shown that a necessary precondition for secure QKD is that sender and receiver can prove the presence of entanglement in the quantum state that is effectively distributed between them. In this contribution, we demonstrate that entanglement witnesses (EW) are powerful tools in order to deliver this entanglement proof. The class of EWs that can be constructed from the available measurements results can be used to provide a necessary and sufficient condition for the existence of quantum correlations. First, we present the set of optimal EWs for two entanglement based (EB) schemes, the 6-state and the 4-state EB protocols. Then, we analyze prepare&measure (P&M) schemes. For this, we investigate the 4-state and the 2-state P&M schemes. For each of these protocols we obtain a reduced set of EWs, yielding a necessary and sufficient condition for the existence of quantum correlations.

Q 33.4 Di 11:30 HU Audimax

Freiraum-Quantenkryptographie — •Nadja Regner[1], Henning Weier[1], Tobias Schmitt-Manderbach[1], Christian Kurtsiefer[2] und Harald Weinfurter[1,3] — [1]Ludwig-Maximilians-Universität München, Schellingstr.4/III 80799 München — [2]Dept. of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542 — [3]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, 85748 Garching

Die Gesetze der Quantenmechanik ermöglichen der Quantenkryptographie einen beweisbar sicheren Schlüsselaustausch für symmetrische Verschlüsselungsalgorithmen. Versucht eine dritte Partei die Verbindung zwischen Alice und Bob zu belauschen, muß sie eine Messung am System vornehmen. Diese Messung läßt das quantenmechnanische System aber nicht unbeeinflußt. Mittels öffentlicher Kommunikation ist es im Nachhinein möglich festzustellen, ob und wieviel Information dem Abhörer maximal zur Verfügung steht. Wir stellen eine freiraumoptische Implementierung des BB84-Protokolls unter Verwendung abgeschwächter Laserpulse vor. Die permanent installierte und selbstjustierende Anlage ermöglicht vollautomatischen und kontinuierlichen Schlüsselaustausch im innerstädtischen Entfernungsbereich (Teststrecke derzeit 500m). Wir berichten von der Inbetriebnahme und ersten Tests, die Aussagen über die Praktikabilität eines freiraumoptischen Quantenkryptographie-Systems zulassen.

Q 33.5 Di 11:45 HU Audimax

Generation of non-classical photon pairs with quantum memory — •Stephanie Manz, Anke Klafs, Dennis Heine, Alois Mair, Thomas Fernholz, Jörg Schmiedmayer und Jian-Wei Pan — Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg

Quantum memories are an important ingredient for long distance quantum communication schemes. We report on experiments towards the realisation of a quantum node, following the DLCZ scheme [1]. A Raman process is used to create non-classical, collective states in hot Rubidium vapour, which can be converted into light. Upon detection of a spontaneously scattered Stokes-photon, we retreive a correlated Anti-Stokes photon after a controllable period of time. Coincidence measurements show a violation of a Cauchy-Schwarz inequality that holds for classical fields.

[1] L.-M. Duan, M. D. Lukin, J. I. Cirac, P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics" Nature 414, 413 (2001)