

1 Schedule

	<i>Tuesday</i>	<i>Wednesday</i>	<i>Thursday</i>	<i>Friday</i>
9:05 - 9:55		Jens Eisert Gaussian states and continuous variables (tutorial)	Tobias Schaetz Towards a Multiplex-Ion Trap Quantum Computer (tutorial)	Valerio Scarani The status of Bell's Inequalities in Quantum Information (tutorial)
9:55 - 10:20		Alessio Serafini Maximal and minimal continuous variable entanglement	Simon Perdrix Around the measurement based quantum computation	Jonathan Ball Exploiting Entanglement in Communication Channels with Correlated Noise
10:20 - 10:45		Peter van Loock Measurements for quantum communication using linear optics	Brendon Lovett Is an optically controlled exciton quantum computer feasible?	Carolina Moura Alves Entanglement detection with non-linear tests
10:45		<i>Coffee</i>	<i>Coffee</i>	<i>Coffee</i>
11:05 - 11:30		Shashank Virmani Simulation of Quantum Measurements and Dynamics with other classes of measurements and Dynamics	John Morton Measuring gate fidelities in electron spin qubit systems using iNC60	Nicolas Brunner Optical telecom networks as weak quantum measurements with post-selection
11:30 - 11:55		Francesco Buscemi Physical realizations of quantum operations	Yuan Liang Lim Photon polarisation entanglement from distant dipole sources	Nikolai Kiesel Experimental observation of three-photon W state
11:55 - 12:20		Joonwoo Bae Power of interaction in quantum search	Ask Dr. Expert part II	Louis-Philippe Lamoureaux Quantum Coin Tossing - An Experimental Approach
12:20		<i>Lunch</i>	<i>Lunch</i>	<i>Lunch</i>
14:00 - 14:50		Antonio Acin QKD I (tutorial)		
14:50 - 15:15		Lluís Masanes QKD II (tutorial)		
15:15	<i>Welcome</i>	<i>Coffee</i>		
15:30 - 15:55	Wolfgang Dür Multipartite Entanglement (tutorial)	Jan Bouda Quantum cryptographic protocols		
15:55 - 16:20		Marcos Curty Entanglement as precondition for secure quantum key distribution		
16:20 - 16:45	Martin Plesch Entangled Graphs	Romain Alléaume Experimental open air Quantum Key Distribution with a single photon source		
16:45 - 17:10	Nick Jones Half's enough: Almost all n party quantum states are completely determined by their n/2+1 party reduced states	Ask Dr. Expert part I		
17:10 - 17:35			Yasser Omar Quantum Information Processing using Particle Statistics	
19:30		<i>Conference Dinner</i>		

2 Participants

<i>Name</i>	<i>Affiliation</i>	<i>Talk</i>
Acin, Antonio (postdoc)	ICFO, Barcelona	QKD tutorial I
Alléaume, Romain (PhD)	Laboratoire de Photonique Quantique et Moléculaire (LPQM) at ENS Cachan	Experimental open air Quantum Key Distribution with a single photon source
Anders, Janet (PhD)	University of Potsdam	-
Aspelmeyer, Markus (postdoc)	Institute for Experimental Physics, University of Vienna	-
Bae, Joonwoo (PhD)	ICFO, Barcelona	Power of interaction in quantum search
Ball, Jonathan (DPhil student)	Centre for Quantum Computation, Clarendon Laboratory, University of Oxford	Exploiting Entanglement in Communication Channels with Correlated Noise
Bertocchi, Guillaume	Université de Nice Sophia-Antipolis Laboratoire de Physique de la Matière Condensée	-
Bouda, Jan (PhD)	Faculty of Informatics, Masaryk University	Quantum cryptographic protocols
Brunner, Nicolas (PhD)	Group of Applied Physics, University of Geneva	Optical telecom networks as weak quantum measurements with post-selection
Buscemi, Francesco (PhD)	Dipartimento di Fisica “A. Volta” Università degli Studi di Pavia	Physical realizations of quantum operations
Cramer, Marcus (PhD)	University of Potsdam	-
Cubitt, Toby (PhD)	Max-Planck-Institute for Quantum Optics, Garching	-
Curty, Marcos (PhD)	Institut für Theoretische Physik I, Universität Erlangen-Nürnberg	Entanglement as precondition for secure quantum key distribution
Dominguez, Alexandre (PhD)	University of Barcelona	-
Dreissig, Julian (PhD)	University of Potsdam	-
Dür, Wolfgang (postdoc)	LMU Munich, Universität Innsbruck	Multipartite Entanglement
Duligall, Joanna (PhD)	University of Bristol	-
Eisert, Jens (postdoc)	University of Potsdam	Gaussian systems and continuous variables
Eckert, Kai (PhD)	Institut fuer Theoretische Physik, Universität Hannover	-
Friedenauer, Axel (PhD)	University of Potsdam	-
Fulconis, Jeremie (PhD)	University of Bristol	-
Garcia, Raul (PhD)	Université Libre de Bruxelles	-
Guehne, Otfried (PhD)	Institut fuer Theoretische Physik, Universität Hannover	-
Guerreau, Olivier (PhD)	GTL-CNRS Telecom Lab, Metz France	-
Hammerer, Klemens (PhD)	Max-Planck-Institute for Quantum Optics, Garching	-
Hein, Marc (PhD)	LMU Munich, Universität Innsbruck	-
Hostens, Erik (PhD)	ESAT-SISTA, KULeuven, Belgium	-
Hyllus, Philipp (PhD)	Institut fuer Theoretische Physik, Universität Hannover	-

Jones, Nick (PhD)	Bristol University	Half's enough: Almost all n party quantum states are completely determined by their $n/2 + 1$ party reduced states
Kaltenbaek, Rainer	Institute for Experimental Physics, University of Vienna	-
Kiesel, Nikolai (PhD)	Max-Planck-Institute for Quantum Optics, Garching	Experimental observation of three-photon W state
Kretschmann, Dennis (PhD)	Technical University of Braunschweig	-
Krueger, Ole (PhD)	Technical University of Braunschweig	-
Lamoureux, Louis-Philippe (PhD)	Université Libre de Bruxelles	Quantum Coin Tossing - An Experimental Approach
Lim, Yuan Liang (PhD)	Quantum Optics and Laser Science group, Blackett Laboratory, Imperial College, London	Photon polarisation entanglement from distant dipole sources
Lovett, Brendon (postdoc)	Department of Materials, Oxford University	Is an optically controlled exciton quantum computer feasible ?
Masanes, Lluís (PhD)	Dept. d'Estructura i Constituents de la Matèria, University of Barcelona	QKD tutorial II
Morton, John (DPhil student)	Department of Materials, University of Oxford	Measuring gate fidelities in electron spin qubit systems using iNC60
Moura Alves, Carolina (PhD)	Clarendon Laboratory, University of Oxford	CQC and Entanglement detection with non-linear tests
Murg, Valentin (PhD)	Max-Planck-Institute for Quantum Optics, Garching	-
Navascués, Miguel (PhD)	ICFO Barcelona	-
Omar, Yasser (postdoc)	Instituto Superior Técnico (Lisbon, Portugal)	Quantum Information Processing using Particle Statistics
Perdrix, Simon (PhD)	LEIBNIZ Laboratory, Grenoble	Around the measurement-based quantum computation
Plesch, Martin (PhD)	Research center for quantum information, Institute of Physics, Slovak Academy of Sciences	Entangled Graphs
Rabl, Peter (PhD)	Universität Innsbruck	-
Reimpell, Michael (PhD)	TU Braunschweig	-
Sauret, Olivier (PhD)	LEPES, CNRS Grenoble	-
Scarani, Valerio (postdoc)	Group of Applied Physics, University of Geneva	The status of Bell's Inequalities in Quantum Information
Schaetz, Tobias (postdoc)	NIST, Boulder	Towards a Multiplex-Ion Trap Quantum Computer
Schnepf, Betina (PhD)	Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe	-
Schuch, Norbert (PhD)	Max-Planck-Institute for Quantum Optics, Garching	-

Serafini, Alessio (PhD)	Dipartimento di Fisica, Università di Salerno INFM UdR Salerno	Maximal and minimal continuous variable entanglement
Van den Nest, Marteen (PhD)	ESAT-SCD Catholic University Leuven	-
van Loock, Peter (postdoc)	Zentrum fuer Moderne Optik (ZEMO) Universitt Erlangen-Nuernberg	Measurements for quantum communication using linear optics
Virmani, Shashank (postdoc)	University of Hertfordshire	Simulation of Quantum Measurements and Dynamics with other classes of measurements and Dynamics
Vollbrecht, Karl G.H. (postdoc)	Max-Planck-Institute for Quantum Optics, Garching	-
Wolf, Michael M. (postdoc)	Max-Planck-Institute for Quantum Optics, Garching	-
Zeier, Robert Michael (PhD)	Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe	-

3 Abstracts

Acin, Antonio :

QKD I (tutorial)

Alléaume, Romain :

Experimental open air Quantum Key Distribution with a single photon source

Key distribution remains a central problem in cryptography, as encryption system security cannot exceed key security. Public key protocols rely on computational difficulty but cannot guarantee unconditional security against future algorithm or hardware advances.

As Bennett and Brassard first proposed twenty years ago, quantum mechanics can be used to build alternative protocols for key distribution. Interest in experimental quantum key distribution (QKD) has evolved from early lab experiments to long distance demonstrations (up to 70 km on telecom fibers and more than 20 km in open air) and now to commercial products. Nevertheless, several technological and theoretical barriers still have to be overcome to improve performance of current QKD systems relying on faint-laser pulses.

Use of a true single photon source presents a significant advantage by potentially permitting greater per-bit extraction of secure information and has recently been implemented in two experiments [1], [2]. Following the work of Beveratos et al, we used single colored NV centers in diamond nanocrystals as a single-photon source and implemented the BB84 scheme on polarized single photons. Quantum communication between Alice and Bob has been realized in open air (at night) between two buildings of the Institut d'Optique. Classical communication necessary for key reconciliation and privacy amplification were realized over the Internet using the software Qucrypt designed by L. Salvail [3].

We present here our experimental results leading to a secure 16 kbit/s exchange rate without attenuation. We also tested attenuation for inferring longer distance performance of our QKD system. We show that the use of a single photon source presents significant advantage over systems relying on faint attenuated laser pulses, in agreement with theoretical models developed to assess QKD security [4].

[1] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.P Poizat, P. Grangier. *Phys. Rev. Lett.* 89 187901(2002)

[2] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto. *Nature*, 420, pp. 762, (2002).

[3] P.M. Nielsen, C. Schori, J.L. Sorensen, L. Salvail, I. Damgard, E. Polzik, *J. Mod. Opt.* 48, 1921 (2001)

<http://www.cki.au.dk/experiment/qcrypto/doc>

[4] N. Lütkenhaus. *Physical Review A*, 61, 052304 (2000).

Bae, Joonwoo :

Power of interaction in quantum search

Alter the quantum search algorithm with at least square-root speedup was known by Grover, it has been developed in some different aspects. One of them is to perform the quantum search through time evolution of proper Hamiltonian. We presented a general description of the Hamiltonian that would perform a quantum search, named as the generalized quantum search Hamiltonian, in [PRA 66, 012314 (2002)]. In this presentation, we show improved speedups beyond the quadratic one due to the interaction of the target state and the others, and the phase alignment between the target state and the final state. We also consider perturbations on quantum search Hamiltonians and then discuss how to save (or correct errors in) a perturbed analog analogue quantum search Hamiltonian. Furthermore, we show a power of the interaction in the quantum adiabatic search algorithm.

Ball, Jonathan :

Exploiting Entanglement in Communication Channels with Correlated Noise

Presentation of a model for a noisy communication channel in which the noise affecting successive transmissions is correlated. The motivation for this model comes from fiber optics and the fluctuation of birefringence in the fiber. Model possesses a high degree of symmetry and it will be shown that the use of entangled input states results in a notably higher classical channel capacity than for the more restricted case of separable states.

Bouda, Jan :

Quantum cryptographic protocols

This talk will give an introduction to the problematics of quantum cryptographic protocols, namely the proof of the impossibility of the unconditionally secure quantum bit commitment and unconditionally secure ideal quantum coin tossing. In the second part of the talk we will present the quantum solutions for the secret sharing and oblivious transfer problem.

Brunner, Nicolas :

Optical telecom networks as weak quantum measurements with post-selection

In this work we establish a link between two apparently unrelated subjects: polarization effects in optical fibers, and the quantum theory of weak measurements. It is shown that the abstract concept of weak measurements followed by post-selection, introduced a decade ago by quantum theorists, naturally appears in the everyday physics of telecom networks. The analogy works as follows. First, polarization mode dispersion (PMD) performs polarization measurements by spatially separating the fiber's eigenmodes. It turns out that the usual telecom limit for PMD, where dispersion has to be minimized, corresponds to the quantum regime of weak measurements. Then polarization dependent losses (PDL) perform post-selection in a very natural way: one post-selects those photons that have not been lost. This is non-trivial physics since the losses depend precisely on the measured degree of freedom: the polarization of light. In case of an infinite PDL (i.e. a polarizer) the post-selection is done on a pure state. For a finite PDL, the post-selection is done on a mixed state. Thus the amount of PDL characterizes the kind of post-selection involved.

Buscemi, Francesco :

Physical realizations of quantum operations

The work covers the problem of unitary dilations of non-unitary quantum evolutions, realized in various ways, referring also to the dilations of quantum dynamical semigroups. Two explicit examples of unitary dilations are given, one related to phase measurement, the other to universal quantum cloning and optimal transposition map.

Curty, Marcos :

Entanglement as precondition for secure quantum key distribution

We demonstrate that a necessary precondition for unconditionally secure quantum key distribution is that sender and receiver can use the available measurement results to prove the presence of entanglement in a quantum state that is effectively distributed between them. One can thus systematically search for entanglement using the class of entanglement witness operators that can be constructed from the observed data. We apply such analysis to two well-known quantum key distribution protocols, namely the 4-state protocol and the 6-state protocol. As a special case, we show that, for some asymmetric error patterns, the presence of entanglement can be proven even for error rates above 25% (4-state protocol) and 33% (6-state protocol).

Dür, Wolfgang :

Multipartite Entanglement (tutorial)

In this tutorial talk I will review basic concepts of bipartite entanglement under the light of possible generalization to multipartite systems. In particular, I will consider equivalence classes of pure states under certain kinds of (local) operations which naturally leads to Schmidt decomposition and to the entanglement measure 'entropy of entanglement' in the bipartite case. Possible generalizations to the multipartite case will be mentioned and several interesting multipartite entangled pure states and their possible applications will be discussed. For mixed states, I will discuss a number of different approaches to classify and quantify multipartite entanglement. Several surprising features such as bound entanglement and its activation will also be considered.

Eisert, Jens :

Gaussian systems and continuous variables (tutorial)

Jones, Nick :

Half's enough: Almost all n party quantum states are completely determined by their $n/2 + 1$ party reduced states

It is known that there exist pure quantum states with irreducible n-party entanglement: their entanglement cannot be reversibly converted into entanglement between less than n parties. Despite the fact that one can find special states with these irreducible correlations at all orders, almost all quantum states are uniquely determined by their lower order correlations. Linden and Woiters have shown that the correlations among at most two thirds of the particles contain all in the information in the state (PRL '02): I provide a tight bound. I've shown that pure states in n parties are nearly always completely determined by their reduced states in $n/2+1$ parties but are not completely determined by their reduced states in less than $n/2$ parties (where each party has the same sized local Hilbert space). Generically the reduced states in $n/2+1$ parties of an n party pure state distinguish it from all other n party pure or mixed states: they act as a sufficient label for the state. This suggests that most quantum states have a reducible quality: their parts can contain as much information as the whole.

Kiesel, Nikolai :

Experimental observation of three-photon W state

We report on the experimental observation of the three-photon polarization-entangled W state using spontaneous parametric down-conversion. This state is inequivalent to the GHZ state under stochastic local operations and classical communications and thus is the representative of the second class of genuine tripartite entanglement. We study the characteristic features of entanglement and demonstrate the high degree of two-photon entanglement in the W state.

Lamoureux, Louis-Philippe :

Quantum Coin Tossing - An Experimental Approach

We discuss the security implications of noise for quantum coin tossing protocols and examine an experimental implementation. In the absence of error correcting codes (as is the case with present day technology), and if significant noise is present, then tossing a single coin becomes problematic. In this case, we are led to consider random n-bit string generation in the presence of noise, rather than single shot coin tossing. We introduce precise security criteria for n-bit string generation and describe an explicit protocol which is being implemented based on the fiber optics "plug and play" quantum cryptosystem. We also discuss possible cheating strategies and state upper bounds on the average bias achievable by a cheater.

Lim, Yuan Liang :

Photon polarisation entanglement from distant dipole sources

It is commonly believed that photon polarisation entanglement can only be obtained via pair creation within the same source or via postselective measurements on photons that overlapped within their coherence time inside a linear optics setup. In contrast to this, we show here that polarisation entanglement can also be produced by distant single photon sources and without the photons ever having to meet, if the detection of a photon does not reveal its origin – the which way information. In the case of two sources, the entanglement arises under the condition of two emissions in certain spatial directions and leaves the dipoles in a maximally entangled state.

Lovett, Brendon :

Is an optically controlled exciton quantum computer feasible ?

I shall discuss the requirements for quantum computing in the context of a scheme based on excitons in solid state nanostructures. The qubit is defined to be the presence or absence of an exciton on a single nanostructure. First, I shall explain my current ideas for performing one and two qubit logic in a pair of such nanostructures using both diagonal and off diagonal coupling in the computational basis - and shall demonstrate that this is feasible within the decoherence time of the device.

I shall then go on to introduce the open problems: is this scheme scalable, and will it be possible to measure the outcome of any computation?

Masanés, Lluís :

QKD tutorial II

It is reviewed the role played by entanglement in QKD, and the parallelism between secret-key and entanglement distillation scenarios. Using this analogy, it is presented an example of Bound Information, a cryptographic analog of bound entanglement, whose existence remained unproven until now.

Morton, John :

Measuring gate fidelities in electron spin qubit systems using iNC60

Characterization of the magnitude of systematic errors in single-qubit logic gates is crucial when evaluating quantum computing implementations. Although the largest-scale quantum computations to date have been implemented using nuclear magnetic resonance (NMR), there are serious problems associated with scaling NMR computations to larger qubit systems. Electron paramagnetic resonance (EPR) offers many parallels to NMR, along with the key advantage that pure groundstates are experimentally accessible. For this reason, EPR has become a key element in a large number of solid state quantum information processing (QIP) proposals. iNC60 provides an electron spin qubit trapped inside a fullerene cage, and benefits from a long decoherence time of up to 240 microseconds.

We have applied pulsed EPR sequences that can be used to amplify different systematic errors in rotations of electron-spin-based qubits, obtaining values for systematic errors in rotation angle and axis in EPR. These values indicate that the fidelities of simple qubit rotations in EPR compare favourably with NMR, and may be further improved through the implementation of error-correcting composite pulse rotations [1]. We conclude that errors in single qubit operations by pulsed EPR are not limiting factors in the implementation of electron-spin-based quantum computers.

[1] H. K. Cummins, G. Llewellyn and J. A. Jones, *PRA*, 67, 042308, 2003

Moura Alves, Carolina :

Entanglement detection with non-linear tests

We present a simple experimental technique that allows testing for entanglement of polarized photons. This test is more powerful than all the Bell-CHSH inequalities taken together. The experimental implementation employs photon bunching and anti-bunching effects.

Omar, Yasser :

Quantum Information Processing using Particle Statistics

I will present examples of how it is possible to do useful and efficient quantum information processing using only the effects of particles statistics, including how these effects can enhance quantum walks with two or more particles.

Perdrix, Simon :

Around the measurement-based quantum computation

One of DiVincenzo's criteria [1] to implement usable qubits for a quantum computer is the ability to perform a universal family of unitary transformations. This criterion comes from the traditional model of quantum computation which is exclusively based on unitary transformations. However there exist some exotic models of quantum computation, like Nielsen's [2,3], which are exclusively based on quantum measurements.

Due to the non-determinism of measurement, and interactions between classical and quantum worlds, an execution using the model introduced by Nielsen is conditional, i.e. each measurement performed depends on the results of the previous ones. Moreover an execution may never end.

It is shown that the Nielsen's scheme can be transformed into a partially unconditional measurement-based model, then into a non-probabilistically ending computational model based on measurement.

[1] D.P. DiVincenzo. *The Physical Implementation of Quantum Computation*. arXiv, quant-ph/0002077

[2] M. A. Nielsen. *Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state*. arXiv, quant-ph/010820, 2001.

[3] D. W. Leung. *Two-qubit projective measurements are universal for quantum computation.* arXiv, quant-ph/0111122.

Plesch, Martin :

Entangled Graphs

Bi-partite entanglement in multi-qubit systems cannot be shared freely. The rules of quantum mechanics impose bounds on how multi-qubit systems can be correlated. The utilization of a concept of "entangled graphs" in order to analyze quantum states of multi-qubit systems is presented. Here qubits are represented by vertexes of the graph while the presence of bi-partite entanglement and/or classical correlation is represented by a specific edge between corresponding vertexes. Existence and possible non-existence of pure/mixed states characterized by a specific graph is examined and general rules are presented. In the second part, the question of a general one-qubit operation estimation is addressed. Recent results are presented and a few open questions are asked.

Scarani, Valerio :

The status of Bell's Inequalities in Quantum Information (tutorial)

A lot of progress has been made, even very recently, in the understanding of the structure of Bell's inequalities applied to quantum physics. But the status of Bell's inequalities in the context of quantum information is still unclear. I will review the known results and stress the unsolved problems whose solution would probably bring us closer to the final picture.

Schaetz, Tobias :

Towards a Multiplex-Ion Trap Quantum Computer (tutorial)

Es wird ein Überblick über die Arbeit der NIST-Gruppe in Bezug auf die Realisierung eines skalierbaren Quantencomputers auf der Basis des Cirac/Zoller'schen Ionenfallenansatzes gegeben. Dabei legen wir den "technischen" Schwerpunkt auf die Demonstration eines Zwei-Qubit Phasengatters (ohne individuelle Adressierung der Einzelionen Qubits), der Verwirklichung der sympathetischen Kühlung in die Nähe des, bzw. in den Grundzustand der Bewegung in der Falle, sowie den Ionen Transport zwischen einzelnen Fallensegmenten. Der "experimentelle" Schwerpunkt liegt auf der Demonstration des Bestehens der Verschränkung zweier Ionen-Qubits nach ihrer örtlicher Separation in verschiedene Fallensegmente, Durchführung einer lokalen Operation und ihrer anschließenden Wiedervereinigung.

Serafini, Alessio :

Maximal and minimal continuous variable entanglement

We provide a meaningful classification of Gaussian states characterizing their entanglement via local and global purities. We introduce maximally and minimally entangled states for given purities and show how they strictly bound the entanglement of Gaussian states. The comparison with finite dimensional instances is briefly addressed. Finally, a possible experimental strategy to directly estimate the logarithmic negativity of 2-mode Gaussian states is suggested.

van Loock, Peter :

Measurements for quantum communication using linear optics

I present a set of criteria to decide whether a given projection measurement can be, in principle, exactly implemented solely by means of linear optics. The linear-optics toolbox may include auxiliary photons, conditional dynamics, phase-space displacements, squeezing transformations, and detection methods such as photon counting and homodyne measurements. I further discuss the extension of this approach to generalized measurements (POVM's).

Virmani, Shashank :

Simulation of Quantum Measurements and Dynamics with other classes of measurements and Dynamics

In quantum information it is common to have situations in which we are restricted to the use of certain classes of operations or measurements. Examples may be experimental, such as restrictions to technologically feasible linear optics devices, or theoretical, such as restriction to LOCC measurements in quantum communication, or restriction to a certain fundamental 'gate set' in both unitary and measurement models of quantum computation. An important

question is therefore how we may emulate other classes of operations and measurements given access to only a certain restricted class. This question is related to classical simulation of quantum systems, and may also be important for noisy implementations of quantum computation. I discuss certain aspects of this very broad problem, the progress that I am aware of, and what remains to be answered.