Secure Communication via Quantum Channels

Bielefeld, Germany, April 24 -28, 2017

Program and Booklet of Abstracts

Organizers:

Holger Boche Christian Deppe Andreas Winter

Monday, April 24th: Information theory

8:45	Gernot Akemann	Welcome Address by a member of ZiFs Board of Directors
8:55	Boche, Deppe, Winter	Introduction by the Convenors
	Session 1 Chair: Andreas Winter	
9:00	Jens Eisert	Tutorium on information theory I
10:30		Coffee Break
11:00	Reinhard Werner	Tutorium on information theory II
12:30		Lunch Break
	Session 2 Chair: Jens Eisert	
13:30	Jiangwei Shang	Convex optimization over SLOCC classes of multipartite entanglement
14:00	David Reeb	Mrs. Gerber's Lemma with quantum side information with an application to cq-polar codes
14:30	Felix Huber	New approaches to the quantum marginal problem
15:00	Ana Sprotte	Steering criteria based on Tsallis entropies
15:30		Coffee Break
	Session 3 Chair: Reinhard F. Werner	
16:00	Cornelia Spee	The maximally entangled set of multipartite quantum states
16:30	Joseph Merrill Renes	Duality of channels and codes: Operational relations between coding and secrecy from quantum mechanics
17:00	Mariami Gachechiladze	Hypergraph states, their entanglement properties, their local unitary equivalences under local Clifford operations and beyond
17:30	Panel Discussion Panel:	Eisert, Gachechiladze, Huber, Reeb, Renes, Shang, Spee, Sprotte

Tuesday, April 25th: Quantum repeater

	Session 1 Chair: Peter van Loock	
8:00	Karol Horodecki	Tutorium on quantum repeaters I
9:30		Coffee Break
10:00	Dieter Meschede	Tutorium on quantum repeaters II
11:30	Infoveranstaltung zur BMBF-Bekanntmachung "Anwendungsszenarien der Quantenkommunikation"	Vorstellung der Bekanntmachung
12:30		Lunch Break
13:30	Infoveranstaltung zur BMBF-Bekanntmachung "Anwendungsszenarien der Quantenkommunikation"	Informationen zur Skizzeneinreichung Erläuterung der administrativen Anforderungen bei der Antragstellung
15:30		Coffee Break
	Session 2 Chair: Dieter Meschede	
16:00	Peter van Loock	Implementations and protocols for the quantum repeater
17:00	Fabian Ewert	Ultrafast fault-tolerant long-distance quantum communication with static linear optics
17:30	Chris Müller	Long distance communication with single photons from Quantum dots
18:00		Coffee Break
	Session 3 Chair: Karol Horodecki	
18:15	Aleksandar Stojanovic	Two layer quantum key establishment over a quantum channel with optical losses
18:45	Timo Holz	Device-independent Secret Key Rates for Quantum Repeater Setups
19:15	Panel Discussion Panel:	Ewert, Holz, Meschede, Müller, Stojanovic, van Loock

Wednesday, April 26th: Information processing with a quantum computer

	Session 1 Chair: Otfried Gühne	
9:00	Christof Wunderlich	Tutorium on quantum computing - Atomic Trapped Ions
10:30		Coffee Break
11:00	Fedor Jelezko	Tutorium on quantum computing II
12:30		Lunch Break
	Session 2 Chair: Christof Wunderlich	
13:30	Caslav Brukner	Quantum controlled order of gates as a resource
14:00	Nicolai Friis	Flexible resources for quantum metrology
14:30	Otfried Gühne	Temporal quantum correlations
15:00		Coffee Break
	Session 3 Chair: Fedor Jelezko	
15:30	Nikolai Miklin	Indistinguishability of causal relations from limited marginals
16:00	Panel Discussion Panel:	Brukner, Friis, Gühne, Miklin, Wunderlich
19:00		Conference Dinner

Thursday, April 27th: Quantum cryptography

	Session 1 Chair: Norbert Lütkenhaus	
9:00	Dagmar Bruß	Tutorium on quantum cryptography I
10:30		Coffee Break
11:00	Harald Weinfurter	Tutorium on quantum cryptography II
12:30		Lunch Break
	Session 2 Chair: Mario Berta	
13:30	Andreas Winter	Hiding information with linear optics against classical adversaries
14:00	Norbert Lütkenhaus	Numerical approaches to QKD security evaluation
14:30	Matej Pivoluska	Layered quantum key distribution
15:00	Anton Trushechkin	New quantum key distribution protocol with pseudorandom bases
15:30		Coffee Break
	Session 3 Chair: Harald Weinfurter	
16:00	Anthony Leverrier	Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction
16:30	Ravishankar Ramanathan	Randomness amplification using nonlocality via local contextuality
17:00	Minglai Cai	Classical - quantum arbitrarily varying wiretap channel
17:30	Mario Berta	Converse bounds for private communication over quantum channels
18:00	Panel Discussion Panel:	Berta, Cai, Leverrier, Lütkenhaus, Pivoluska, Ramanathan, Trushechkin, Yang

Friday, April 28th: Methods of quantum optics

	Session 1 Chair: Marcus Huber	
9:00	Nicolas Cerf	Tutorium on methods of quantum optics I
10:30		Coffee Break
11:00	Christine Silberhorn	Tutorium on methods of quantum optics II
12:30		Lunch Break
	Session 2 Chair: Nicolas Cerf	
13:30	Marcus Huber	Experimental certification of high dimensional quantum entanglement
14:00	Ludovico Lami	Schur complements and matrix means in quantum optics
14:30	Andrey Moskalenko	Subcycle approach to quantum optics
15:00		Coffee Break
	Session 3 Chair: Christine Silberhorn	
15:30	Krishnakumar Sabapathy	On non-Gaussian operations on light: photon-added Gaussian channels
16:00	Evan Meyer-Scott	Experimental violations of Bells inequality: present and future
16:30	Vladyslav C. Usenko	Nonclassical light in quantum cryptography
17:00	Ali Asadian	Heisenberg-Weyl Observables: Bloch vectors in phase space
17:30	Panel Discussion Panel:	Cerf, Huber, Lami, Meyer-Scott, Moskalenko, Sabapathy, Usenko

SECURE COMMUNICATION VIA QUANTUM CHANNELS

Quantum Communication offers the possibility of an inherently safe transmission, which is based on qualitatively novel physical principles: namely, the wave-particle duality in quantum mechanics, and the possibility of quantum-mechanical entanglement.

It thus offers the possibility to directly implement security in a communication system through embedded security. Point-to-point transmission distances have already been implemented. Quantum technology is the coming technology, which has already motivated various national and European research funding institutions to carry out large-scale projects, for example the quantum technologies program, and the "Flagship Quantum Technologies", which is of course also involved in the DFG.

It is therefore particularly important to bring together the scientists from the different fields that are relevant to quantum technologies in order to advance the progress of the joint work. Our conference will be an elementary step in this direction. We deal with the following topics, all of which are directly relevant to the problem of safe communication via quantum channels.

- Quantum information theory
- Quantum repeater
- Information processing with a quantum computer
- Quantum cryptography
- Methods of quantum optics

INFORMATIONSVERANSTALTUNG ZUR BMBF-BEKANNTMACHUNG “ANWENDUNGSSZENARIEN DER QUANTENKOMMUNIKATION”

Das Bundesministerium für Bildung und Forschung (BMBF) beabsichtigt die Förderung der Erforschung und Entwicklung von Technologien für eine langreichweitige glasfaserbasierte Quantenkommunikation, die den Stand der Forschung und Technologie dem Einsatz in praxistauglichen Kommunikationssystemen wesentlich näher bringt. Um Lösungsansätze der Quantenkommunikation im Hinblick auf die Tauglichkeit für künftige Anwendungen evaluieren zu können, ist der Aufbau von Testinfrastrukturen und -systemen sowie die Durchführung von Testmessungen erforderlich. Gefördert werden soll daher ein (ggf. zwei) Verbundvorhaben mit dem Ziel, eine glasfaserbasierte Demonstratorstrecke für die Quantenkommunikation mittels Quantenrepeatern aufzubauen.

Bei der Förderung kommen der engen Zusammenarbeit von Unternehmen und Forschungseinrichtungen im universitären und außeruniversitären Bereich, der Anbindung kleiner und mittlerer Unternehmen sowie der nachhaltigen Stärkung der Wertschöpfungsketten am Standort Deutschland besondere Bedeutung zu. Die Fördermaßnahme erfolgt im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit “Selbstbestimmt und sicher in der digitalen Welt”.

Auf der Informationsveranstaltung werden die Bekanntmachung vorgestellt und Informationen zur Skizzeneinreichung gegeben sowie die administrativen Anforderungen bei der Antragstellung erläutert. Anschließend stehen Mitarbeiter des Projektträgers VDI/VDE Innovation + Technik GmbH für Fragen und weiterführende Gespräche zur Verfügung.

Weitere Informationen:

http://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/quantenkommunikation

HEISENBERG-WEYL OBSERVABLES: BLOCH VECTORS IN PHASE SPACE

Ali Asadian

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

We introduce a Hermitian generalization of Pauli matrices to higher dimensions which is based on Heisenberg-Weyl operators. The complete set of Heisenberg-Weyl observables allows us to identify a real-valued Bloch vector for an arbitrary density operator in discrete phase space, with a smooth transition to infinite dimensions. Furthermore, we derive bounds on the sum of expectation values of any set of anti-commuting observables. Such bounds can be used in entanglement detection and we show that Heisenberg-Weyl observables provide a first non-trivial example beyond the dichotomic case.

Ref:Phys. Rev. A 94, 010301(R)(2016)

CONVERSE BOUNDS FOR PRIVATE COMMUNICATION OVER QUANTUM CHANNELS

Mario Berta

California Institute of Technology
1200 E California Blvd
Pasadena CA 91125
USA

We establish a converse bounds on the private transmission capabilities of a quantum channel. The main conceptual development builds firmly on the notion of a private state, which is a powerful, uniquely quantum method for simplifying the tripartite picture of privacy involving local operations and public classical communication to a bipartite picture of quantum privacy involving local operations and classical communication. This approach has previously led to some of the strongest upper bounds on secret key rates, including the squashed entanglement and the relative entropy of entanglement. Here we use this approach along with a "privacy test" to establish a general meta-converse bound for private communication.

QUANTUM CONTROLLED ORDER OF GATES AS A RESOURCE

Caslav Brukner

Quantum Optics, Quantum Nanophysics, Quantum Information
Boltzmanngasse 5
1090 Wien
Austria

Quantum computation is standardly assumed to happen on a definite causal structure, where the order of the gates in a circuit is fixed in advance and is independent of the states. However, the interplay between general relativity and quantum mechanics might require to consider more general situations in which the metric, and hence the causal structure, is indefinite. Quantum computation on such structures would allow the order in which the gates are applied to be controlled by a quantum state, and analogously quantum communication would allow the direction of communication between parties to be controlled by a quantum state. I will show that these new resources make possible solving specific computational and communication complexity problems more efficiently than any causally ordered quantum circuit.

TUTORIUM QUANTUM CRYPTOGRAPHY

Dagmar Bruß

Heinrich-Heine-Universität Düsseldorf
Institut für Theoretische Physik III
Universitätsstraße 1, Gebäude 25.32
D-40225 Düsseldorf

Quantum cryptography employs quantum mechanical properties for cryptographic tasks. A famous example is quantum key distribution (QKD), where two parties aim at establishing a common secret random key. This tutorial offers an introduction into various QKD protocols and the physical principles underlying the security of QKD. In a historical overview of security proofs we will touch concepts such as "unconditional security" and "epsilon-security". An essential figure of merit for QKD protocols and their practical implementations is the secret key rate, for which we will discuss some examples. Finally, a recent extension to quantum key distribution between more than two parties will be presented.

CLASSICAL - QUANTUM ARBITRARILY VARYING WIRETAP CHANNEL

Minglai Cai

Technische Universität München
Lehrstuhl für Theoretische Informationstechnik
80290 München

We analyze arbitrarily varying classical-quantum wiretap channels.These channels are subject to two attacks at the same time: one passive (eavesdropping), and one active (jamming). We progress on previous works by introducing a reduced class of allowed codes that fulfills a more stringent secrecy requirement than earlier definitions. In addition, we prove that non-symmetrizability of the legal link is suficient for equality of the deterministic and the common randomness assisted secrecy capacities. At last, we focus on analytic properties of both secrecy capacities: We completely characterize their discontinuity points, and their super-activation properties.

TUTORIUM QUANTUM OPTICS

Nicolas Cerf

QuIC - Ecole Polytechnique de Bruxelles
Universit Libre de Bruxelles
50 av. F. D. Roosevelt - CP 165/59
B-1050 Bruxelles
Belgique

I will introduce the basic notions of quantum optics, starting with the correspondence principle, the description of the quantum state of a mode of the light field in Fock space, and the definition of the bosonic field operator, number operator, and quadrature operators. I will then go over the most usual states (coherent, squeezed, thermal, number states) and operators (displacement, rotation, squeezing operators), and address the photon counting statistics and correlation function. I will summarize the representation of the light field in phase space (P, Q, and Wigner functions) and move on to the symplectic formalism, suitable for the description of Gaussian states and operators in terms of displacement vector and covariance matrix. I will illustrate this formalism for the special cases of a beam splitter and two-mode squeezer (non-degenerate parametric amplifier), and will complete the description of the Gaussian set with the notion of homodyne and heterodyne measurements, as well as the Williamson and Bloch-Messiah decompositions. After some quick introduction to the entropy in state space (von Neumann entropy) and phase space (Wehrl entropy) and if time allows I will present some standard applications of continuous-variable quantum information processing, such as Gaussian quantum teleportation and quantum cloning. Finally, I will briefly discuss entanglement of continuous-variable states (EPR variance, Duan-Simon entanglement criterion).

TUTORIUM QUANTUM INFORMATION

Jens Eisert

Freie Universität Berlin
Fachbereich Physik
Arnimallee 14
14195 Berlin-Dahlem

In this tutorial, I will review basic notions in quantum information theory, to lay the foundations for the later tutorials. In the focus of the tutorial are notions of entanglement - bi-partite and multi-partite - of quantum channels and their various capacities, hinting at questions of privacy.

ULTRAFAST FAULT-TOLERANT LONG-DISTANCE QUANTUM COMMUNICATION WITH STATIC LINEAR OPTICS

Fabian Ewert

Johannes Gutenberg-Universität Mainz
Saarstr. 21
55122 Mainz

We present an in-depth analysis regarding the error resistance and optimization of our all-optical Bell measurement and ultrafast long-distance quantum communication scheme proposed in [arXiv:1503.06777]. In order to promote our previous proposal from loss- to fault-tolerance, we introduce a general and compact formalism that can also be applied to other related schemes (including non-all-optical ones such as [PRL 112, 250501]). With the help of this new representation we show that our communication protocol does not only counteract the inevitable photon loss during channel transmission, but is also able to resist common experimental errors such as Pauli-type errors (bit- and phase-flips) and detector inefficiencies (losses and dark counts). Furthermore, we demonstrate that on the physical level of photonic qubits the choice of the standard linear optical Bell measurement with its limited efficiency is optimal for our setting in the sense that, apart from their potential use in state preparation, more advanced Bell measurements yield only a small decrease in resource consumption. We devise two state generation schemes that provide the required ancillary encoded Bell states (quasi-)on-demand at every station. The schemes are either based on nonlinear optics or on linear optics with multiplexing and exhibit resource costs that scale linearly or less than quadratic with the number of photons per encoded qubit, respectively. Finally, we show that it is possible to operate our communication scheme with on-off detectors instead of employing photon-number-resolving detectors.

FLEXIBLE RESOURCES FOR QUANTUM METROLOGY

Nicolai Friis

Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Boltzmanngasse 3
1090 Wien
Austria

Quantum metrology offers a quadratic advantage over classical approaches to parameter estimation problems by utilizing entanglement and non-classicality. However, the hurdle of actually implementing the necessary quantum probe states and measurements, which vary drastically for different metrological scenarios, is usually not taken into account. We show that for a wide range of tasks in metrology, 2D cluster states (a particular family of states useful for measurement-based quantum computation) can serve as flexible resources that allow one to efficiently prepare any required state for sensing, and perform appropriate (entangled) measurements using only single qubit operations. Crucially, the overhead in the number of qubits is less than quadratic, thus preserving the quantum scaling advantage. This is ensured by using a compression to a logarithmically sized space that contains all relevant information for sensing. We specifically demonstrate how our method can be used to obtain optimal scaling for phase and frequency estimation in local estimation problems, as well as for the Bayesian equivalents with Gaussian priors of varying widths.

[1] N. Friis, D. Orsucci, M. Skotiniotis, P. Sekatski, V. Dunjko, H. J. Briegel, and W. Dür, e-print arXiv:1610.09999 [quant-ph] (2016).

HYPERGRAPH STATES, THEIR ENTANGLEMENT PROPERTIES, THEIR LOCAL UNITARY EQUIVALENCES UNDER LOCAL CLIFFORD OPERATIONS AND BEYOND

Mariami Gachechiladze

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

Hypergraph states form a family of multiparticle quantum states that generalizes cluster states and graph states. We study the action and graphical representation of nonlocal unitary transformations between hypergraph states. This leads to a generalization of local complementation and graphical rules for various gates, such as the CNOT gate and the Toffoli gate. As an application we show that already for five qubits local Pauli operations are not sufficient to check local equivalence of hypergraph states. Furthermore, we use our rules to construct entanglement witnesses for three-uniform hypergraph states.

TEMPORAL QUANTUM CORRELATIONS

Otfried Gühne

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

Sequential measurements on a single particle play an important role in fundamental tests of quantum mechanics. We provide a general method to analyze temporal quantum correlations, which allows us to compute the maximal correlations for sequential measurements in quantum mechanics. As an application, we present the full characterization of temporal correlations in the simplest Leggett-Garg scenario and in the sequential measurement scenario associated with the most fundamental proof of the Kochen-Specker theorem.

DEVICE-INDEPENDENT SECRET KEY RATES FOR QUANTUM REPEATER SETUPS

Timo Holz

Heinrich-Heine-Universität Düsseldorf
Institut für Theoretische Physik III
Universitätsstraße 1, Gebäude 25.32
D-40225 Düsseldorf

The device-independent approach to quantum key distribution (QKD) aims to distribute a secret key between two or more parties with untrusted devices, possibly under full control of a quantum adversary. The performance of a QKD-protocol can be quantified by the secret key rate R, which can be lower-bounded via the violation of an appropriate Bell-inequality. We study secret key rates in the device-independent bipartite case for different quantum repeater setups and compare them to their device-dependent analogon [1]. The quantum repeater setups under consideration are the original protocol by Briegel et al. [2] and the hybrid quantum repeater protocol by van Loock et al. [3]. For a given repeater scheme and a given QKD-protocol, the secret key rate depends on a variety of parameters, such as the gate quality or the fidelity of initially distributed states. We investigate the impact of these parameters and suggest optimized strategies.

[1] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bru??, Phy. Rev. A 87, 052315 (2013)
[2] H. J. Briegel, W. D??r, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. 81, 5932 (1998)
[3] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. 96, 240501 (2006)

NEW APPROACHES TO THE QUANTUM MARGINAL PROBLEM

Felix Huber

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

he quantum marginal problem asks: Given a set of marginals, does there exist a corresponding joint state? Here, we approach this compatibility problem using the weight enumerator machinery known from quantum error correcting codes. In particular, we generalise the so-called shadow enumerators, which were introduced by Rains, to higher local dimensions. We draw connections to monogamy relations, which constrain the possible correlations present in multipartite quantum systems.

With this, we provide new bounds on the existence of absolutely maximally entangled states and on quantum error correcting codes in general.

EXPERIMENTAL CERTIFICATION OF HIGH DIMENSIONAL QUANTUM ENTANGLEMENT

Marcus Huber

Institute for Quantum Optics and
Quantum Information
Austrian Academy of Sciences
Boltzmanngasse 3
A-1090 Vienna
Austria

High-dimensional entanglement offers promising perspectives in quantum information science. In practice, however, the main challenge is to devise efficient methods to characterize high-dimensional entanglement, based on the available experimental data which is usually rather limited. Here we report the characterization and certification of high-dimensional entanglement in photon pairs, encoded in temporal modes. Building upon recently developed theoretical methods, we certify an entanglement of formation of 2.09(7) ebits in a time-bin implementation, and 4.1(1) ebits in an energy-time implementation. These results are based on very limited sets of local measurements, which illustrates the practical relevance of these methods.

TUTORIUM QUANTUM REPEATER

Karol Horodecki

University of Gdansk
Faculty of Mathematics, Physics and Informatics
Wydzial Matematyki, Fizyki i Informatyki
ul. Wita Stwosza 57
80-308 Gdansk
Poland

A major application of quantum communication is the distribution of entangled particles for use in quantum key distribution. Owing to noise in the communication line, quantum key distribution is, in practice, limited to a distance of a few hundred kilometres, and can only be extended to longer distances by use of a quantum repeater, a device that performs entanglement distillation and quantum teleportation. The existence of noisy entangled states that are undistillable but nevertheless useful for quantum key distribution raises the question of the feasibility of a quantum key repeater, which would work beyond the limits of entanglement distillation, hence possibly tolerating higher noise levels than existing protocols. Here we exhibit fundamental limits on such a device in the form of bounds on the rate at which it may extract secure key. As a consequence, we give examples of states suitable for quantum key distribution but unsuitable for the most general quantum key repeater protocol.

TUTORIUM QUANTUM COMPUTER

Fedor Jelezko

Universität Ulm
Institut für Quantenoptik
Albert-Einstein-Allee 11
D-89081 Ulm

Over the past several decades, quantum information science has emerged to seek answers to the question: can we gain some advantage by storing, transmitting and processing information encoded in systems that exhibit unique quantum properties? Today it is understood that the answer is yes, and many research groups around the world are working towards the highly ambitious technological goal of building a quantum computer, which would dramatically improve computational power for particular tasks. A number of physical systems, spanning much of modern physics, are being developed for quantum computation. However, it remains unclear which technology, if any, will ultimately prove successful. Here we describe the latest developments for each of the leading approaches and explain the major challenges for the future.

SCHUR COMPLEMENTS AND MATRIX MEANS IN QUANTUM OPTICS

Ludovico Lami

Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain

Gaussian states and Gaussian operations are of primary interest in quantum optics, due to the ease of their practical implementations. Remarkably, the quadratic nature of the correlations displayed by these states makes matrix analysis tools suitable for their analysis. This work exploits this connection to prove novel results in quantum optics.- We derive fundamentalconstraints for the Schur complement of positive matrices, whichprovide an operatorstrengthening to recently established information inequalities for quantumcovariance matrices, including strongsubadditivity. As an application, we establish fundamental properties of a recently proposed Gaussian steerability measure [Phys. Rev. Lett.114, 060403 (2015)]. - Since the correlations exhibited by Gaussian states are quadratic by definition, natural quantifiers of those are based on Rnyi-2 entropies. We show that the Rnyi-2 mutual information of a bipartite Gaussian state is lower bounded by twice its Rnyi-2 Gaussian entanglement of formation (R2 EoF), an inequality that fails to hold for conventional von Neumann entropies. An important consequence of this inequality is the monogamy of the R2 EoF, here established for the first time. Perhaps surprisingly, this entanglement measure has been recently conjectured to be connected to cryptographic quantifiers [Phys. Rev. Lett.117, 240505 (2016)].

SECURITY OF CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION: TOWARDS A DE FINETTI THEOREM

Anthony Leverrier

INRIA Paris - Projet Secret
2 rue Simone Iff CS 42112
75589 Paris Cedex 12
France

Establishing the security of continuous-variable quantum key distribution against general attacks in a realistic finite-size regime is an outstanding open problem in the field of theoretical quantum cryptography if we restrict our attention to protocols that rely on the exchange of coherent states. Indeed, techniques based on the uncertainty principle are not known to work for such protocols, and the usual tools based on de Finetti reductions only provide security for unrealistically large block lengths. We address this problem here by considering a new type of Gaussian de Finetti reduction, that exploits the invariance of some continuous-variable protocols under the action of the unitary group $U(n)$ (instead of the symmetric group S_n as in usual de Finetti theorems), and by introducing generalized $SU(2,2)$ coherent states. Our reduction shows that it is sufficient to prove the security of these protocols against Gaussian collective attacks in order to obtain security against general attacks, thereby confirming rigorously the widely held belief that Gaussian attacks are indeed optimal against such protocols.

NUMERICAL APPROACHES TO QKD SECURITY EVALUATION

Norbert Lütkenhaus

Institute for Quantum Computing
Department of Physics & Astronomy
University of Waterloo
200 University Ave W
Waterloo, ON N2L 3G1
Canada

Bound secret information is classical information that contains secrecy but from which secrecy cannot be extracted. The existence of bound secrecy has been conjectured but is currently unproven, and in this work we provide analytical and numerical evidence for its existence. Specifically, we consider two-way post-processing protocols in prepare-and-measure quantum key distribution based on the well-known six-state signal states. In terms of the quantum bit-error rate Q of the classical data, such protocols currently exist for $Q < \frac{55}{\sqrt{10}} \approx 27.6\%$. On the other hand, for Q13 no such protocol can exist as the observed data is compatible with an intercept-resend attack. This leaves the interesting question of whether successful protocols exist in the interval $\frac{55}{\sqrt{10}} \leq Q < \frac{1}{3}$. Previous work has shown that a necessary condition for the existence of two-way post-processing protocols for distilling secret key is breaking the symmetric extendability of the underlying quantum state shared by Alice and Bob. Using this result, it has been proven that symmetric extendability can be broken up to the 27.6% lower bound using the advantage distillation protocol. In this work, we first show that to break symmetric extendability it is sufficient to consider a generalized form of advantage distillation consisting of one round of post-selection by Bob on a block of his data. We then provide evidence that such generalized protocols cannot break symmetric extendability beyond 27.6%. We thus have evidence to believe that 27.6% is an upper bound on two-way post-processing and that the interval $\frac{55}{\sqrt{10}} \leq Q < \frac{1}{3}$ is a domain of bound secrecy.

TUTORIUM QUANTUM REPEATER

Dieter Meschede

Institut für Angewandte Physik
Wegelerstr. 8
D-53115 Bonn

Quantum repeaters are conceptually promising to establish long distance quantum communication by overcoming the distance limits imposed by attenuation and noise in optical fibers for point to point quantum links. The tutorial will present an overview about the schemes and building blocks required for establishing quantum repeaters and the experimental challenges that need to be solved in order to render quantum repeaters successful.

EXPERIMENTAL VIOLATIONS OF BELLS INEQUALITY: PRESENT AND FUTURE

Evan Meyer-Scott

University of Paderborn
Warburger Straße 100
33098Paderborn

Bells inequality provides a limit to the correlations possible in local realistic theories. Quantum mechanics predicts stronger correlations, but only recently have these stronger correlations been observed with a reasonably minimal set of experimental assumptions. I will present two experiments related to violations of Bells inequality. In the first part of the talk I will present the "loophole-free Bell inequality violation using entangled photon pairs from the National Institute of Standards and Technology (USA), and compare our results with other experiments using photons, nitrogen-vacancy centres, and atoms.

One of the key challenges we overcome is photon loss: Bells inequality can only be violated with entangled photon pairs when the total transmission and detection probability is greater than 2/3. This strongly limits the achievable distance for such a violation. In the second part of the talk I will thus present work on what a future long-distance Bell inequality violation could look like, using the technique of photonic qubit precertification. Here the presence of the photon arriving at the receiver is probed locally, and the Bell test proceeds only after successful certification, removing the effect of channel losses. To perform this certification, we split the arriving photon in two via parametric down-conversion, and detect one photon of the pair while mapping the qubit state to the other. I will discuss a first experiment that shows this photonic qubit precertification procedure indeed preserves the quantum states of photons and provides a path toward implementations of advanced quantum communication over many kilometres.

INDISTINGUISHABILITY OF CAUSAL RELATIONS FROM LIMITED MARGINALS

Nikolai Miklin

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

We investigate the possibility of distinguishing among different causal relations starting from a limited set of marginals. Our main tool is the notion of adhesivity, that is, the extension of probability or entropies defined only on subsets of variables, which provides additional independence constraints among them. Our results provide a criterion for recognizing which causal structures are indistinguishable when only limited marginal information is accessible. Furthermore, the existence of such extensions greatly simplifies the characterization of a marginal scenario, a result that facilitates the derivation of Bell inequalities both in the probabilistic and entropic frameworks, and the identification of marginal scenarios where classical, quantum, and postquantum probabilities coincide.

LONG DISTANCE COMMUNICATION WITH SINGLE PHOTONS FROM QUANTUM DOTS

Chris Müller

Humboldt-Universität zu Berlin
Institut für Physik, AG Nanooptik
Newtonstraße 15
12489 Berlin

Quantum information offers a possible means of overcoming many challenges including the development of quantum communication and quantum computation [1]. Quantum communication requires suitable quantum networks consisting of quantum nodes. These quantum nodes are necessary to generate, save, and process the quantum state locally. Such a node, for example, could be realized by using an atom or quantum dot, with the information encoded at an atomic transition wavelength and transmitted by optical fibers. However, these atomic transitions are not at telecom wavelengths for which losses in optical fibers are minimal. The resulting losses are prohibitively high for long distance communication between nodes. Here we present two basic approaches to overcoming this problem via quantum hybrid systems.

The first approach is a two-color entangled photon pair source [2]. We achieve this by using nonlinear crystal in a folded-sandwich configuration to generate pairs of entangled photons with different wavelengths via spontaneous parametric down conversion. Presently, this source produces signal and idler photons with highly non-degenerated wavelengths, while obtaining an entanglement fidelity of $75 \pm 2\%$. These entangled photons can be used to interface two different quantum systems to create a quantum hybrid system.

The second approach uses frequency conversion in a nonlinear crystal to convert the quantum information to telecom wavelength [3]. We stabilized a quantum dot to emit at the caesium D1 line (894 nm). These quantum dot photons are then converted via difference frequency generation to a 1557 nm photon to reduce losses in optical fibers.

[1] Kimble, Nature, 453, 1023 (2008)

[2] Dietz et al., Applied Physics B, 122, 33 (2016)

[3] Zaske et al., Phys. Ref. Let. 109, 147404 (2012)

SUBCYCLE APPROACH TO QUANTUM OPTICS

Andrey Moskalenko

Department of Physics
Mailbox 686
University of Konstanz

Squeezed states of electromagnetic radiation have quantum fluctuations below those of the vacuum field. They offer a unique resource for quantum information systems and precision metrology, including gravitational wave detectors, which require unprecedented sensitivity. Since the first experiments on this non-classical form of light, quantum analysis has been based on homodyning techniques and photon correlation measurements. These methods currently function in the visible to near-infrared and microwave spectral ranges. They require a well-defined carrier frequency, and photons contained in a quantum state need to be absorbed or amplified. Quantum non-demolition experiments may be performed to avoid the influence of a measurement in one quadrature, but this procedure comes at the expense of increased uncertainty in another quadrature. Here we generate mid-infrared time-locked patterns of squeezed vacuum noise. After propagation through free space, the quantum fluctuations of the electric field are studied in the time domain using electro-optic sampling with few-femtosecond laser pulses. We directly compare the local noise amplitude to that of bare (that is, unperturbed) vacuum. Our nonlinear approach operates off resonance and, unlike homodyning or photon correlation techniques, without absorption or amplification of the field that is investigated. We find subcycle intervals with noise levels that are substantially less than the amplitude of the vacuum field. As a consequence, there are enhanced fluctuations in adjacent time intervals, owing to Heisenbergs uncertainty principle, which indicate generation of highly correlated quantum radiation. Together with efforts in the far infrared, this work enables the study of elementary quantum dynamics of light and matter in an energy range at the boundary between vacuum and thermal background conditions.

LAYERED QUANTUM KEY DISTRIBUTION

Matej Pivoluska

Institute for Quantum Optics and
Quantum Information
Austrian Academy of Sciences
Boltzmanngasse 3
A-1090 Vienna
Austria

In usual security proofs of quantum protocols the adversary (Eve) is expected to have full control over any quantum communication between any communicating parties (Alice and Bob). Eve is also expected to have full access to an authenticated classical channel between Alice and Bob. Unconditional security against any attack by Eve can be proved even in the realistic setting of device and channel imperfection. In this paper we show that the security of quantum key distribution protocols is ruined if one allows Eve to possess a very limited access to the random sources used by Alice. Such knowledge should always be expected in realistic experimental conditions via different side channels.

RANDOMNESS AMPLIFICATION USING NONLOCALITY VIA LOCAL CONTEXTUALITY

Ravishankar Ramanathan

Centre for Quantum Technologies
National University of Singapore
Block S15, 3 Science Drive 2
Singapore 117543
China

Recently the first physically realistic protocol amplifying the randomness of Santha-Vazirani sources using a finite number of no-signaling devices and with a constant rate of noise has been proposed, however there still remained the open question whether this can be accomplished under the minimal conditions necessary for the task. Namely, is it possible to achieve randomness amplification using only two no-signaling devices and in a situation where the violation of a Bell inequality implies only an upper bound for some outcome probability for some setting combination? Here, we solve this problem and present the first device-independent protocol for the task of randomness amplification of Santha-Vazirani sources using a device consisting of only two non-signaling components. We show that the protocol can amplify any such source that is not fully deterministic into a totally random source while tolerating a constant noise rate and prove the security of the protocol against general no-signaling adversaries. The minimum requirement for a device-independent Bell inequality based protocol for obtaining randomness against no-signaling attacks is that every no-signaling box that obtains the observed Bell violation has the conditional probability $P(\mathrm{x}|\mathrm{u})$ of at least a single input-output pair (u, x) bounded from above. We show how one can construct protocols for randomness amplification in this minimalistic scenario.

MRS. GERBER'S LEMMA WITH QUANTUM SIDE INFORMATION WITH AN APPLICATION TO CQ-POLAR CODES

David Reeb

Zentrum Mathematik, M5
Technische Universität München
Boltzmannstrasse 3
85748 Garching

"Bounds on information combining" are entropic inequalities that determine how the information (entropy) of a set of random variables can change when these are combined in certain prescribed ways. Such bounds play an important role in classical information theory, particularly in coding and Shannon theory; entropy power inequalities are special instances of them. The arguably most elementary kind of information combining is the addition of two binary random variables (a CNOT gate), and the resulting quantities play an important role in Belief propagation and Polar coding. We investigate this problem in the setting where quantum side information is available, which has been recognized as a hard setting for entropy power inequalities.

Our main technical result is a non-trivial, and close to optimal, lower bound on the combined entropy, which can be seen as an almost optimal "quantum Mrs. Gerber's Lemma". Our proof uses three main ingredients: (1) a new bound on the concavity of von Neumann entropy, which is tight in the regime of low pairwise state fidelities; (2) the quantitative improvement of strong subadditivity due to Fawzi-Renner, in which we manage to handle the minimization over recovery maps; (3) recent duality results on classical-quantum-channels due to Renes et al. We furthermore present conjectures on the optimal lower and upper bounds under quantum side information, supported by interesting analytical observations and strong numerical evidence.

We finally apply our bounds to Polar coding for binary-input classical-quantum channels, and show the following three results: (A) Even non-stationary channels polarize under the polar transform. (B) The blocklength required to approach the symmetric capacity scales at most sub-exponentially in the gap to capacity. (C) Under the aforementioned lower bound conjecture, a blocklength polynomial in the gap suffices.

DUALITY OF CHANNELS AND CODES: OPERATIONAL RELATIONS BETWEEN CODING AND SECRECY FROM QUANTUM MECHANICS

Joseph Merrill Renes

Institut für Theoretische Physik
Wolfgang-Pauli-Str. 27
8093 Zürich
Switzerland

For any given channel W with classical inputs and possibly quantum outputs, a dual classical-input channel $W^{\perp}$ can be defined by embedding the original into a channel N with quantum inputs and outputs. Here we give new uncertainty relations for a general class of entropies that lead to very close relationships between the original channel and its dual. Moreover, we show that channel duality can be combined with duality of linear codes, whereupon the uncertainty relations imply that the performance of a given code over a given channel is entirely characterized by the performance of the dual code on the dual channel. This has several applications. In the context of polar codes, it implies that the rates of polarization to ideal and useless channels must be identical. Duality also relates the tasks of channel coding and privacy amplification, implying that the finite blocklength performance of extractors and codes is precisely linked, and that optimal rate extractors can be transformed into capacity-achieving codes, and vice versa. Finally, duality also extends to the EXIT function of any channel and code. Here it implies that for any channel family, if the EXIT function for a fixed code has a sharp transition, then it must be such that the rate of the code equals the capacity at the transition. This may give a different route to proving a code family achieves capacity by establishing sharp EXIT function transitions.

ON NON-GAUSSIAN OPERATIONS ON LIGHT: PHOTON-ADDED GAUSSIAN CHANNELS

Krishnakumar Sabapathy

Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain

We present a framework for studying bosonic non-Gaussian channels of continuous-variable systems. Our emphasis is on a class of channels that we call photon-added Gaussian channels which are experimentally viable with current quantum-optical technologies. A strong motivation for considering these channels is the fact that it is compulsory to go beyond the Gaussian domain for numerous tasks in continuous-variable quantum information processing like entanglement distillation from Gaussian states and universal quantum computation. The single-mode photon-added channels we consider are obtained by using two-mode beamsplitters and squeeze operators with photon addition applied to the ancilla ports giving rise to families of non-Gaussian channels. For each such channel, we derive its operator-sum representation, indispensable in the present context. We observe that these channels are Fock-preserving (coherence non-generating). We then report two novel examples of activation using our scheme of photon addition, that of nonclassicality at outputs of channels that would otherwise output only classical states, and of both the quantum and private capacities, hinting at far-reaching applications for quantum-optical communication. Further, we see that noisy Gaussian channels can be expressed as a convex mixture of these non-Gaussian channels. We also present other physical and information-theoretic properties of these channels.

CONVEX OPTIMIZATION OVER SLOCC CLASSES OF MULTIPARTITE ENTANGLEMENT

Jiangwei Shang

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

As the fundamental feature of quantum mechanics, entanglement has found its application in numerous quantum information processing tasks. A bipartite state is entangled if it cannot be written as a convex sum of product states. For more than two parties, the characterization becomes more complicated as there exist different classes of multipartite entanglement. One strategy utilizes the notion of stochastic local operations and classical communication (SLOCC). In this talk, I will present two reliable algorithms for convex optimization over any defined SLOCC entanglement classes. The first algorithm uses a simple gradient approach, while the other one employs the recently introduced accelerated projected-gradient (APG) method. In both algorithms, the quantum constraints are ensured by using the Gilberts algorithm. For demonstration, the algorithms are applied to the likelihood ratio test which serves as a good benchmark for quantifying the weight of evidence for entanglement with limited data, but is usually very hard to compute.

TUTORIUM QUANTUM OPTICS

Christine Silberhorn

Universität Paderborn
Fakultät für Naturwissenschaften
Department Physik - Angewandte Physik
33095 Paderborn

Classical optical networks have been widely used to explore a broad range of transfer phenomena based on coherent interference of waves, which relate to different disciplines in physics, information science, and even biological systems. At the quantum level, the quantized nature of light, this means the existence of photons and entangled states, gives rise to genuine quantum effects that can appear completely counter-intuitive. Yet, to date, quantum network experiments typically remain very limited in terms of the number of photons, reconfigurability and, maybe most importantly, network size and dimensionality.

Photonic quantum systems, which comprise multiple optical modes as well as highly non-classical and sophisticated quantum states of light, have been investigated intensively in various theoretical proposals over the last decades. However, their implementation requires advanced setups of high complexity, which, to date, poses a considerable challenge on the experimental side. The successful realization of controlled quantum network structures is key for many applications in quantum optics and quantum information science.

THE MAXIMALLY ENTANGLED SET OF MULTIPARTITE QUANTUM STATES

Cornelia Spee

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

Entanglement is a resource under the restriction of operations to Local Operations assisted by Classical Communication (LOCC). In the bipartite case the optimal resource is well known and corresponds to a single state, i.e. the maximally entangled state. In the multipartite case the optimal resource under LOCC among pure fully entangled states corresponds in general to a whole set of states, the Maximally Entangled Set (MES). The MES is the minimal set of pure n-partite states with the property that any pure truly n-partite entangled state can be obtained deterministically via LOCC from a state within this set [1]. We investigated the MES for three-qubit [1], four-qubit [1,2] and generic three-qutrit states [3] and showed that the MES is of measure zero for three-qubit states, whereas it is of full measure in the case of four qubits and three qutrits. This is due to the fact that for four qubits and three qutrits non-trivial deterministic LOCC transformations among pure states which are entangled among all parties and dimensions are hardly ever possible. For generic three-qutrit and four-qubit states we identified the measure-zero subset of states in the MES which can be deterministically converted via a non-trivial LOCC protocol to some pure state which is entangled among all parties and dimensions. These states are the most relevant ones for deterministic entanglement manipulation. Moreover, we identified transformations among pure three-qutrit states that are possible via separable maps but not via LOCC. We also considered the practical scenario of local operations assisted by finitely many rounds of classical communication and studied pure state transformations for a general class of states of arbitrarily many subsystems and arbitrary dimensions [4]. In this context we also investigated the MES under the restriction to finite round LOCC protocols.

[1] J.I. de Vicente, C. Spee, and B. Kraus, Phys. Rev. Lett. 111, 110502 (2013).

[2] C . Spee, J.I. de Vicente, and B. Kraus, J. Math. Phys. 57, 052201 (2016).

[3] M. Hebenstreit, C. Spee, and B. Kraus, Phys. Rev. A 93, 012339 (2016).

[4] C. Spee, J.I. de Vicente, D. Sauerwein, and B. Kraus, Phys. Rev. Lett. 118, 040503 (2017); J.I. de Viceqnte, C. Spee, D. Sauerwein, and B. Kraus, Phys. Rev. A 95, 012323 (2017).

STEERING CRITERIA BASED ON TSALLIS ENTROPIES

Ana Sprotte

Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen

EPR-steering is a term coined by Schrodinger in 1935, within the context of Einstein-Podolsky-Rosen (EPR) argument to name Alice's ability in affecting Bob's state through her choice of measurement basis. Steering has been formalized in terms of a quantum information task involving bipartite states and measurement settings, in which case the existence of entanglement is necessary but not suficient. It has also been shown that steerability of any assemblage can always be formulated as a joint measurability problem. Steering inequalities based on entropic uncertainty relations have been proposed and experimentally tested in the last years. Based on Tsallis entropies, we present a generalization for the entropic steering and its connection with known results from the literature. Special attention will be given for certain families of Tsallis entropies, in order to show that the violation of these generalized criteria can detect more steerable states than others proposed in the literature, considering the scenario of few measurements and general two-qubit states.

TWO LAYER QUANTUM KEY ESTABLISHMENT OVER A QUANTUM CHANNEL WITH OPTICAL LOSSES

Aleksandar Stojanovic

Department of Mathematics
IST
Technical University of Lisbon
1049-001 Lisboa
Portugal

The rapid increase on the information sharing around the world, leads to an utmost requirement for capacity and bandwidth. However, the need for security in the transmission and storage of information is also of major importance. The use of quantum technologies provides a practical solution for secure communications systems. Quantum key distribution (QKD) was the first practical application of quantum mechanics, and nowadays it is the most developed one. In order to share secret keys between two parties can be used several methods of encoding. Due to its simplicity, the encoding into polarization is one of the most used. However, when we use optical fibers as transmission channels, the polarization suffers random rotations that may change the state of polarization (SOP) of the light. Thus, in order to enable real-time communication using this encoding method it is required to make use of a dynamic control system. We describe a scheme of quantum information transmission, which is based on the polarization encoding, allowing to share secret keys through optical fibers without interruption. The dynamic polarization control system used for compensation of depolarization in such scheme is described, both theoretically and experimentally. Its advantages and limitations for the use in quantum communications are presented and discussed. Another actual problem in QKD is authentication of classical messages through a quantum channel with losses. The aim of the authentication protocol is to guarantees the identity of legitimate users, avoiding the man-in-the-middle attack. An authentication protocol requires an initially shared secret and it can be realized by software or by a physical system. In the first case a pseudo-random number generator (PRNG) is used while in the second case synchronized optical chaotic systems can be employed. In this direction, the present work considers both cases, taking into account the influence of optical losses in a quantum channel. Firstly, we show how to implement an authenticated polarizationbased B92 QKD protocol using a PRNG. Its security is analyzed taking into account the number of bits of the pre-shared secret. Following, we describe a chaos-based authenticated B92 QKD protocol: We consider a chaotic system whose output is a light polarization state that changes chaotically, solving the problem of synchronization of two of such systems at the same time. The Stokes parameter S1 of the output field is used to obtain a pseudo-random bit sequence that is relevant to implement the authentication. We emphasize functional limits for these two implementations. Additional system parametrization has been provided, increasing already obtained high security level of proposed QKD system based on B92 protocol. Furthermore, new QKD schemes on physical level are proposed, which fit even better additional parametrization. One of future implications of those results may be obtaining more advanced optical QKD layer, which could be more independent from actual electronics.

NEW QUANTUM KEY DISTRIBUTION PROTOCOL WITH PSEUDORANDOM BASES

Anton Trushechkin

Steklov Mathematical Institute
Russian Academy of Sciences
Gubkina 8
Moscow 119991
Russia

We present a QKD protocol of a new type and analyse its security against the intercept-resend attack. The specific feature of this protocol is the use of pseudorandom bases. This allows one to avoid sifting and, hence, loss of a half of the raw key. We prove that this protocol gives better secret key rates than the BB84 protocol and approximately the same rates as the asymmetric BB84 protocol. Also we consider the problem of breaking pseudorandom sequences of quantum states and show that it is closely related to the problem of quantum state discrimination.

NONCLASSICAL LIGHT IN QUANTUM CRYPTOGRAPHY

Vladyslav C. Usenko

Department of Optics
Palacky University
17. listopadu 12
77146 Olomouc
Czech Republic

Quantum key distribution (QKD) is an essentially quantum task allowing two trusted parties to share secure cryptographic keys. It is well known that coherent states are in principle sufficient for QKD. However, numerous practical imperfections limit the performance of QKD protocols and may impose requirements on nonclassicality of the signal states. We will therefore address the role of nonclassicality of quantum signals in QKD and reveal some of the regimes when it is crucially required as well as some cases when it can be surprisingly harmful.

IMPLEMENTATIONS AND PROTOCOLS FOR THE QUANTUM REPEATER

Peter van Loock

Quanten-, Atom- und Neutronenphysik
Johannes Gutenberg-Universität
Institut für Physik
Staudingerweg 7
D 55128 Mainz

The original solution to the problem of long-distance quantum communication by Briegel, Dür, Cirac, and Zoller is based on short-distance distributions of entangled states, their long-distance connection by teleportation (entanglement swapping), and the detection of transmission and operational errors by additional local gates and classical communication (entanglement purification). The probabilistic nature of quantum error detection in this case requires the entangled states to be storable and the classical communication to be two-way.

The probably most prominent proposal for an actual implementation of the original quantum repeater concept is that of Duan, Lukin, Cirac, and Zoller (DLCZ). It marked a major leap forward in at least two aspects. On the protocol side, it no longer required any additional rounds of entanglement purification based on local quantum logic. Instead, the detection of transmission loss errors was automatically built into the initial entanglement distribution (and so was the light-memory quantum transfer) and the detection of memory loss errors was automatically built into the entanglement swapping steps. On the physical level, DLCZ relied upon a collective-spin encoding of many atoms coupled to an optical mode in free space and the processing of these optical modes by linear optics only. Though in principle scalable to large distances, the DLCZ scheme, operating in the limit of very low excitations, leads to rather small repeater rates. As a remedy, possible variations of DLCZ have been proposed as well as distinct approaches involving the use of continuous quantum variables. Typically, these latter approaches would still be based on some nonlinear light-matter interactions such as those obtainable in Cavity-QED.

We shall first give an overview over some of the approaches to realize the above standard type of quantum repeater. Then we will also discuss the more recent developments in quantum repeater research in which probabilistic quantum error detection is (partially or entirely) replaced by deterministic quantum error correction and thus the necessity of quantum memories may be (partially or entirely) circumvented.

TUTORIUM QUANTUM CRYPTOGRAPHY

Harald Weinfurter

Ludwig-Maximilians-Universität München
Department für Physik
Schellingstr. 4/III
D-80799 München

Quantum key distribution (QKD) allows two parties to exchange a secure key for cryptography using the quantum mechanical properties of light. We have achieved QKD over the record distance of 144 km, which is representative for a link to a low orbit satellite. In this context we also demonstrated that a key exchange with a fast moving device is possible by establishing a QKD link to an aircraft at a distance of 20 km to the ground station. Our current research focuses on the implementation of a compact transmitter suited for handheld user devices, where we plan to combine light from a laser diode array with laser written waveguides on a glass chip.

TUTORIUM QUANTUM INFORMATION

Reinhard F. Werner

Institut für Theoretische Physik
Leibniz Universität Hannover
Appelstraße 2
30167 Hannover

Quantum Information is concerned with the study of quantum mechanics from the point of view of information theory, as well as with the use of quantum mechanical systems for the purpose of information processing and computation. On the one hand, this includes quantum information theory, with topics such as quantum teleportation, the transmission of information through quantum channels, quantum cryptography, and the quantification of quantum entanglement as a resource for the aforementioned tasks. On the other hand, it involves quantum computation, i.e., computation based on the laws of quantum mechanics, covering topics such as quantum algorithms, quantum error correction, and the physical realization of quantum computers.

HIDING INFORMATION WITH LINEAR OPTICS AGAINST CLASSICAL ADVERSARIES

A. Winter

Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain

Cryptography arises from the information theoretic tension between players with different amounts of power to access or process information. One of the most basic questions is that of discriminating two hypothesis (i.e. recover one bit of information) using either a 'strong' set of measurements (decision rules) with a 'weak' one. Here we discuss such a scenario inspired by quantum optics, so-called Gaussian operations and classical computation (GOCC) [Takeoka/Sasaki, PRA 78:022320, 2008]: Not very surprisingly, GOCC cannot distinguish optimally even two coherent states of a single mode [Takeoka/Sasaki, PRA 78:022320]. We find states, each a mixture of multi-mode coherent states, which are almost perfectly distinguishable by suitable measurements, but when restricted to GOCC, i.e. linear optics and post-processing, the states appear almost identical. The construction is random and relies on coding arguments and phase space methods. Open questions include whether there one can give a constructive version of the argument, and whether for instance even Gaussian states could be used, or how efficient the hiding is.

TUTORIUM QUANTUM COMPUTER - ATOMIC TRAPPED IONS

Christof Wunderlich

Lehrstuhl Quantenoptik
Department Physik - Fakultät IV
Universität Siegen
D-57068 Siegen

Trapped atomic ions are a well-advanced physical system for quantum information science (QIS). QIS is meant to encompass the quest for a universal, or specialized processor for quantum information, the investigation of fundamental questions of quantum physics, as well as applications of techniques emanating from these investigations to other fields (for example, precision spectroscopy). In this tutorial I introduce essential elements of the physics relevant for trapped atomic ions when they are used for state-of-the-art experiments in QIS paying particular attention to quantum computing. It will be outlined how suitably chosen internal states of individual laser-cooled atomic ions confined in a Paul trap provide well-isolated qubits that can be initialized and measured individually. A collection of ions forms a Coulomb crystal and an interaction between individual ions, a prerequisite for conditional quantum dynamics, is mediated by the ions external (motional) degrees of freedom through Coulomb interaction. Electromagnetic fields are employed to coherently prepare individual qubits. For conditional quantum gates, optical forces associated with the field driving an internal resonance (acting on the ions motional states) allow for coupling internal and motional states in usual ion traps. Alternatively, magnetic gradient induced coupling (MAGIC) yielding a qubit-phonon or qubit-qubit interaction can be used for conditional quantum gates making it possible to exclusively use radio-frequency fields for any coherent operation. After introducing the physics background relevant for ion trap quantum computing, I will give an overview of the current status by way of some exemplary experiments.

LIST OF PARTICIPANTS

1. Gernot Alber
   Institut für Angewandte Physik
   Hochschulstraße 4a
   64289 Darmstadt
   Tel.: +49-6151/16-20400
   gernot.alber@physik.tu-darmstadt.de

2. Vahid Ansari
   Universität Paderborn
   Fakultät für Naturwissenschaften
   33095 Paderborn
   Tel: +49 5251 60-5884
   vahid.ansari@uni-paderborn.de

3. Ali Asadian
   Universität Siegen
   Department Physik
   Emmy-Noether-Campus
   Walter-Flex-Straße 3
   57068 Siegen
   Tel: +49 271 740 3531
   asadian@physik.uni-siegen.de

4. Mario Berta (Talk)
   California Institute of Technology
   1200 E California Blvd
   Pasadena CA 91125
   USA
   Tel: +1 6263958762
   berta@caltech.edu

5. Philippe Blanchard
   Fakultät für Physik
   Universität Bielefeld
   Postfach 10 01 31
   D-33501 Bielefeld
   Tel: +49 521 / 106-6205
   blanchard@Physik.Uni-Bielefeld.DE

6. Holger Boche (Organizer)
   Technische Universität München
   Lehrstuhl für Theoretische Informationstechnik
   80290 München
   Tel.: +49 (89) 289 - 23241
   boche@tum.de

7. Caslav Brukner
   Quantum Optics, Quantum Nanophysics
   Boltzmanngasse 5
   1090 Wien
   Tel: +43 (01) 4277 72582
   caslav.brukner@univie.ac.at

8. Dagmar Bruß (Tutorial Speaker, Support)
   Heinrich-Heine-Universität Düsseldorf
   Institut für Theoretische Physik III
   Universitätsstraße 1, Gebäude 25.32
   D-40225 Düsseldorf
   Tel.: +49 211 81-10679
   dagmar.bruss@uni-duesseldorf.de

9. Minglai Cai
   Technische Universität München
   Lehrstuhl für Theoretische Informationstechnik
   80290 München
   minglai.cai@tum.de

10. Nicolas Cerf (Tutorial Speaker)
    QuIC - Ecole Polytechnique de Bruxelles
    Universit Libre de Bruxelles
    50 av. F. D. Roosevelt - CP 165/59
    B-1050 Bruxelles
    Belgique
    Tel: +32-2-650 28 58
    ncerf@ulb.ac.be

11. Ana Cristina Sprotte Costa
    Universität Siegen
    Department Physik
    Walter-Flex-Straße 3
    57068 Siegen
    Tel: +49 271 740 3799
    ana.costa@physik.uni-siegen.de

12. Christian Deppe (Organizer)
    Universität Bielefeld
    Fakultät für Mathematik
    Postfach 10 01 31
    D - 33615 Bielefeld
    Tel.: +49 (0)521 106-4790
    cdeppe@math.uni-bielefeld.de

13. Kristian Döbrich
    Kommunikationssysteme
    VDI/VDE Innovation + Technik GmbH
    Steinplatz 1
    10623 Berlin
    Tel. +49 (0) 30 310078-345
    kristian.doebrich@vdivde-it.de

14. Christof Eigner
Universität Paderborn
Fakultät für Naturwissenschaften
33095 Paderborn
Tel.: +49 5251 60-5896
christof.eigner@uni-paderborn.de

15. Jens Eisert (Tutorial Speaker)
Freie Universität Berlin
Fachbereich Physik
Arnimallee 14
14195 Berlin-Dahlem
Tel.: +49-(0)30-838-54781
jenseisert@googlemail.com

16. Fabian Ewert (Talk)
Johannes Gutenberg-Universität Mainz
Saarstr. 21
55122 Mainz
Tel.: +49 6131 39-0
ewertf@uni-mainz.de

17. Matthias Florian
Institut for Theoretical Physics
University of Bremen
P.O. Box 330 440
28334 Bremen
Tel: +49 421 218-62047
mflorian@itp.uni-bremen.de

18. Nicolai Friis (Talk)
Institute Quantum Optics & Information
Austrian Academy of Sciences
Boltzmanngasse 3
1090 Wien
Austria
Tel: +43 512 507 52224
Nicolai.Friis@uibk.ac.at

19. Mariami Gachechiladze (Talk)
Universität Siegen
Department Physik
Walter-Flex-Straße 3
57068 Siegen
Tel: +49 271 740 3716
marigachi@physik.uni-siegen.de

20. Mara Garca
Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain
mariaschmetterling9@gmail.com

21. Otfried Gühne
Universität Siegen
Department Physik
Walter-Flex-Straße 3
57068 Siegen
otfried.Gühne@uni-siegen.de¿

22. Thorsten Haase
Institut für Angewandte Physik
Hochschulstraße 4a
64289 Darmstadt
thorsten.haase@stud.tu-darmstadt.de

23. Jan Philipp Höpker
Universität Paderborn
Fakultät für Naturwissenschaften
Department Physik - Angewandte Physik
33095 Paderborn
hoeppi@mail.uni-paderborn.de

24. Timo Holz
Heinrich-Heine-Universität Düsseldorf
Institut für Theoretische Physik III
Universitätsstraße 1, Gebäude 25.32
D-40225 Düsseldorf
Tel.: +49 211 81-10679
timoholz89@web.de

25. Karol Horodecki (Tutorial Speaker)
University of Gdansk
Faculty of Mathematics, Physics and Informatics
Wydzial Matematyki, Fizyki i Informatyki
ul. Wita Stwosza 57
80-308 Gdansk
Poland
Tel: +48 58 523 22 87
karol.horodecki@inf.ug.edu.pl

26. Marcus Huber (Talk)
Institute for Quantum Optics and
Quantum Information
Austrian Academy of Sciences
Boltzmanngasse 3
A-1090 Vienna
Austria
Tel.: (+ 43 1) 4277
marcus.huber@univie.ac.at

27. Felix Huber (Talk)
Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen
Tel: +49 271 740 3716
felix.huber@physik.uni-siegen.de

28. Gisbert Janssen (Talk)
Technische Universität München
Fakultät für Elektrotechnik und Informationstechnik
Theresienstraße 90
80333 München
Tel.: +49 (89) 289 - 23247
gisbert.janssen@tum.de

29. Fedor Jelezko (Tutorial Speaker)
Universität Ulm
Institut für Quantenoptik
Albert-Einstein-Allee 11
D-89081 Ulm
Tel: ++ 49 / 731 / 50-23750
fedor.jelezko@uni-ulm.de

30. Hermann Kampermann
Heinrich-Heine-Universität Düsseldorf
Institut für Theoretische Physik III
Universitätsstrae 1, Gebäude 25.32
D-40225 Düsseldorf
Hermann.Kampermann@hhu.de

31. Zahra Khanian
Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain
zbkhanian@gmail.com

32. Karsten-Kai König
Institut für Theoretische Physik
Leibniz Universität Hannover
Appelstraße 2
30167 Hannover
Tel: +49 (0)511 762-17496
karsten.koenig@stud.uni-hannover.de

33. Ludovico Lami (Talk)
Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain
ludovico.lami@gmail.com

34. Anthony Leverrier
INRIA Paris - Projet Secret
2 rue Simone Iff CS 42112
75589 Paris Cedex 12
+33 (0)1 80 49 42 23
anthony.leverrier@inria.fr

35. Norbert Lütkenhaus (Talk)
Institute for Quantum Computing
Department of Physics & Astronomy
University of Waterloo
200 University Ave W
Waterloo, ON N2L 3G1
Canada
Tel: +1-519-888-4567 X 32870
nlutkenhaus@uwaterloo.ca

36. Frederik Lohoff
Institut for Theoretical Physics
University of Bremen
P.O. Box 330 440
28334 Bremen
Tel: +49 421 218-62047
flohoff@itp.uni-bremen.de

37. Michael Lynch-White
School of Physics & Astronomy
University of St Andrews
North Haugh
St Andrews, KY16 9SS
Scotland
UK
Tel: +44 1334 463128
mplw@st-andrews.ac.uk

38. Dieter Meschede (Tutorial Speaker)
Institut für Angewandte Physik
Wegelerstr. 8
D-53115 Bonn
Tel: +49 228 73-3477
meschede@iap.uni-bonn.de

39. Evan Meyer-Scott (Talk)
University of Paderborn
Warburger Straße 100
33098Paderborn
Tel: (+49) 5251 60-5882
evan.meyer.scott@upb.de

40. Nikolai Miklin (Talk)
Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen
Tel: +49 271 740 3531
nikolai.miklin@student.uni-siegen.de

41. Chris Müller (Talk)
Humboldt-Universität zu Berlin
Institut für Physik, AG Nanooptik
Newtonstraße 15
12489 Berlin
Tel: +49 (0)30 2093-4826
chrism@physik.hu-berlin.de

42. Deepak Pandey
Institut für Angewandte Physik
Wegelerstr. 8
D-53115 Bonn
Tel: +49 228 73-6580
d.pandey@iap.uni-bonn.de

43. Laura Padberg
Fakultät für Naturwissenschaften
Department Physik - Angewandte Physik
33095 Paderborn
laura-p@mail.upb.de

44. Carsten Petersen
Fakultät für Physik
Universität Bielefeld
Postfach 10 01 31
D-33501 Bielefeld
Tel: +49 521 / 106-4775
carsten@physik.uni-bielefeld.de

45. Matej Pivoluska
Institute for Quantum Optics and
Quantum Information
Austrian Academy of Sciences
Boltzmanngasse 3
A-1090 Vienna
Austria
Tel.: (+ 43 1) 4277
pivoluskamatej@gmail.com

46. Ravishankar Ramanathan (Talk)
Centre for Quantum Technologies
National University of Singapore
Block S15, 3 Science Drive 2
Singapore 117543
China
ravishankar.r.10@gmail.com

47. Kai Redeker
LMU München
Faculty of Physics
AG Weinfurter
Schellingstraße 4/III
D-80799 München
Tel: +49 89 2180-6934
Kai.Redeker@physik.uni-muenchen.de

48. David Reeb (Talk) Zentrum Mathematik, M5
Technische Universität München
Boltzmannstrasse 3
85748 Garching
David Reeb ¡reeb.qit@gmail.com¿
Tel: +49 89 289-18409
(Quantum Cryptography)

49. Joseph Merrill Renes (Talk)
Institut für Theoretische Physik
Wolfgang-Pauli-Str. 27
8093 Zürich
Switzerland
Tel: +41 44 633 70 62
renes@itp.phys.ethz.ch

50. Andrey Moskalenko (Talk)
Department of Physics
Mailbox 686
University of Konstanz
Tel: +49 7531 88 3811
andrey.moskalenko@uni-konstanz.de

51. Krishnakumar Sabapathy (Talk)
Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain
krishnakumar.sabapathy@gmail.com

52. David Sabonis
Niels Bohr Institute
University of Copenhagen
H. C. Orsted Institute
Universitetsparken 5
2100 Copenhagen O
Denmark
deividassab@gmail.com

53. Matteo Santandrea
Applied Physics
Integrated Quantum Optics
Universität Paderborn
Warburgerstraße 100
33098 Paderborn
Tel.: +49 (5251) 60 5880
matteo.santandrea@upb.de

54. Alexander Sauer
Institut für Angewandte Physik
Hochschulstraße 4a
64289 Darmstadt
alexander.sauer@lea.tu-darmstadt.de

55. Rene Schwonnek
Institut für Theoretische Physik
Leibniz Universität Hannover
Appelstraße 2
30167 Hannover
Tel: +49 (511) 76217498
rene.schwonnek@itp.uni-hannover.de

56. Sajad Saeedinaeeni
Technische Universität München
Lehrstuhl für Theoretische Informationstechnik
80290 München
Tel.: +49 (89) 289 - 23251
sajad.saeedinaeeni@tum.de

57. Jiangwei Shang (Talk)
Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen
jiangwei.shang@quantumlah.org
Tel: +49 271 740 3531

58. Christine Silberhorn (Tutorial Speaker)
Universität Paderborn
Fakultät für Naturwissenschaften
Department Physik - Angewandte Physik
33095 Paderborn
Tel: +49 5251 60-5884
christine.silberhorn@upb.de

59. Cornelia Spee (Talk)
Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen
Spee@physik.uni-siegen.de

60. Aleksandar Stojanovic (Talk)
Department of Mathematics
IST
Technical University of Lisbon
1049-001 Lisboa
Portugal
stojanovic.alex1@gmail.com

61. Ulrich Tamm
Fachhochschule Bielefeld
Fachbereich Wirtschaft und Gesundheit
Postfach 10 11 13
33511 Bielefeld
ulrich.tamm@fh-bielefeld.de

62. Johannes Tiedau
University of Paderborn
Integrated Quantum Optics
Warburger Strasse 100
D-33098 Paderborn
Tel.: +49 (5251) 60 5868
johannes.tiedau@uni-paderborn.de

63. A. S. Trushechkin (Talk)
Steklov Mathematical Institute
Russian Academy of Sciences
Gubkina 8
Moscow 119991
Russia
trushechkin@mi.ras.ru

64. Vladyslav C. Usenko (Talk)
Department of Optics
Palacky University
17. listopadu 12
77146 Olomouc
Czech Republic
Tel. +420585634248
usenko@optics.upol.cz

65. Peter van Loock
Quanten-, Atom- und Neutronenphysik
Johannes Gutenberg-Universität
Institut für Physik
Staudingerweg 7
D 55128 Mainz
Tel.: +49 6131 39-23628
loock@uni-mainz.de

66. Felix Weber
Institut für Angewandte Physik
Hochschulstraße 4a
64289 Darmstadt
felix.weber@physik.tu-darmstadt.de

67. Harald Weinfurter (Tutorial Speaker)
Ludwig-Maximilians-Universität München
Department für Physik
Schellingstr. 4/III
D-80799 München
Tel: + 49 (0)89 2180-2044
harald.weinfurter@physik.uni-muenchen.de

68. Reinhard F. Werner (Tutorial Speaker)
Institut für Theoretische Physik
Leibniz Universität Hannover
Appelstraße 2
30167 Hannover
Tel: +49 (0)511 762-17501
Fax: +49 (0)531 762-17499
reinhard.werner@itp.uni-hannover.de

69. Andreas Winter (Organizer)
Universitat Autònoma de Barcelona
Quantum Information Group
Physics Department
Ed. C, 08193 Bellaterra (Barcelona)
Spain
andreas.winter@uab.cat

70. Christof Wunderlich (Tutorial Speaker)
Lehrstuhl Quantenoptik
Department Physik - Fakultät IV
Universität Siegen
D-57068 Siegen
Tel: +49-271-740
christof.wunderlich@uni-siegen.de

71. Nikolai Wyderka
Universität Siegen
Department Physik
Emmy-Noether-Campus
Walter-Flex-Straße 3
57068 Siegen
Tel: +49 271 740 3716
wyderka@physik.uni-siegen.de

72. Dong Yang (Talk)
China Jiliang University
Hangzhou
Zhejiang 310018
China
dyang@cjlu.edu.cn