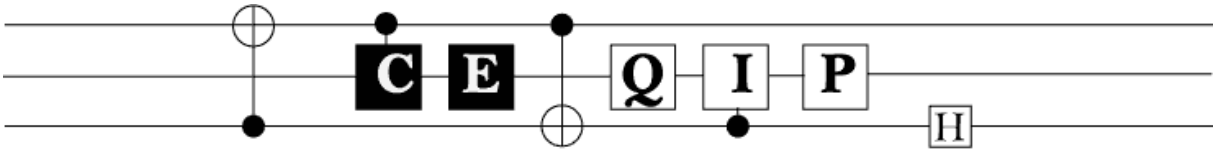
Central European Quantum Information Processing Workshop

Jindřichuv Hradec, Czech Republic
June 1st - 4th, 2009



Visegrad Group

http://www.quniverse.org/ceqip/

QAIP

CEQIP

CEQIP'09 (Central European Quantum Information Procesing) is focused on current challenges and paradigms of quantum information processing. The selected topics for this year are: quantum protocols, quantum dynamics, quantum algorithms and computation, quantum tomography.

Conference venue:
The workshop (and registration) will take place in the conference hall of Museum of Jindřichuv Hradec located close St.John the Baptist Church, what allows us to preserve the traditionally stimulating scientific atmosphere.

About Jindřichuv Hradec:
Jindrichuv Hradec is a cute Gothic and Renaissance town in South Bohemia. It is among the most significant tourist destinations in the Czech Republic. Its center has been declared a historical conservation area for its exquisite historical, architectural, and cultural sights including an extensive castle complex.

Social program: The workshop is planned to be conducted in a very nice and stimulating athmosphere with an intensive quantum scientific program and a classical social program (see program for details). It will include the visit of the castle and a conference dinner in the historic music pavillion Roundel (see pictures bellow). The Roundel is situated in a small garden with arcades on the ground floor level and it may be used for garden feasts in favourable weather. The social program is completely covered by the conference fee (also for accompying persons).

Steering Committee:
⋆ Vladimír Bužek (RCQI, Bratislava & FI MU, Brno)
⋆ Jozef Gruska (FI MU, Brno)

Organizing Committee:
⋆ Jan Bouda (FI MU, Brno)
⋆ Martin Plesch (RCQI, Bratislava & Quniverse)
⋆ Mário Ziman (RCQI, Bratislava & FI MU, Brno)

Program Committee:
Andris Ambainis, Vladimír Bužek, Jozef Gruska, Simon Perdrix, Denes Petz, Mário Ziman, Karol Zyczkowski

Invited speakers:
⋆ Giacomo Mauro D'Ariano (Pavia)
⋆ Jens Eisert (Potsdam)
⋆ Nobuyuki Imoto (Osaka)
⋆ Hai-Woong Lee (Daejeon)
⋆ Serge Massar (Brussels)
⋆ Karol Zyckowski (Krakow)

Support:
Visegrad Fundation (`http://www.visegradfund.org/`)
EU project QAP (`http://www.qubitapplications.com/`)
Project MSM0021622419

Visegrad Group QAP

INVITED TALKS

1. *Giacomo Mauro D'Ariano*
(University of Pavia, Pavia, Italy)
The quantum comb: theory and applications to quantum networks

I will present a method for optimizing a quantum circuit for a given task. The method is based on the powerful notion of "quantum comb", which describes a circuit board in which one can insert variable subcircuits. Mathematically it corresponds to a generalization of the notions of quantum operation and POVM. The method allows to address new kinds of quantum processing tasks, and represents the canonical route to quantum estimation and to optimization of quantum circuits in general, beyond the classic approach of Helstrom and Holevo. Using comb theory it is possible to find the optimal network arrangement of the multiple uses of a unknown input channels, providing the solution of long-standing problems, such as the optimal quantum tomography setup, or the optimal storing- retrieving of unitaries—the quantum version of algorithm learning. The method allows to prove equivalence of arrangements for optimal estimation of unitaries, and the need of memory assisted protocols for for optimal discrimination of memory channels. The latter also leads to a new notion of distance for channels with memory, generalizing the usual cb-norm distance of channels. Optimization of oracle- discrimination provides a systematic way to address some problems of optimal quantum algorithms. Finally, the quantum comb is the appropriate mathematical formulation of the single-party strategy in a multi-party quantum protocol, including quantum games and cryptography. For example it provides a very synthetic formulation of the Quantum Bit Commitment and its impossibility proof, and allows to proof general statements about multi-round protocols, such as the optimal alignment of reference frames based on quantum communication.

2. *Jens Eisert*
(University of Potsdam, Potsdam, Germany)
Too entangled to be useful?

It is often argued that entanglement is at the root of the speedup for quantum compared to classical computation, and that one needs sufficient entanglement for this speedup to be manifest. In measurement-based quantum computing (MBQC), the need for a highly entangled initial state is particularly obvious. In this work we show that, remarkably, quantum states can be too entangled to be useful for the purpose of computation. What is more, we can prove that this phenomenon occurs for the dramatic majority of all states: the fraction of pure states on n qubits not subject to the problem is smaller than e^{-n^2}. Our results show that computational universality is actually a rare property in quantum states. For the proof we establish a link between the "quantum probabilistic method" and ideas on quantum many-body systems. This work highlights a new aspect of the question concerning the role entanglement plays for quantum computational speed-ups. We will also present a new classification of primitives that can be used in order to systematically construct new models for measurement-based computation.

[1] D. Gross, S. Flammia, J. Eisert, Phys. Rev. Lett. 102 (2009).
[2] D. Gross, J. Eisert, Phys. Rev. Lett. 98, 220503 (2007).

3. *Nobuyuki Imoto*
(Osaka University, Osaka, Japan)
Backaction control in quantum measurement and anomalous weak value in an interferometer

It is well known that a two-qubit gate can be realized by an idealized quantum nondemolision (QND) gate. In spite of its name "nondemolision", it cannot be used to look inside of an interferometer due to its measurement back action [1]. It is possible, however, to control the strength of the measurement, and doing so, one can accomplish a weak limit of measurement, in which the expected values can be measured inside an interferometer without affecting the interference. Aharonov [2] predicted anomalous weak values in several cases, which is especially striking in the Hardy's interferometer [3]. Experimentally, this can be done by "joint" weak measurement. Using a photon version of Hardy's paradox, these anomalous values have been actually measured [4]. In my talk I will introduce this topic in conjunction with our recent research activity [5].

[1] N. Imoto et.al, Phys.Rev.A 32, 2287 (1985).
[2] Y. Aharonov et al., Phys. Lett. A 301, 130 (2002).
[3] L. Hardy, Phys. Rev. Lett. 68, 2981 (1992).
[4] K. Yokota et.al, New J. Phys. 11, 033011(2009).
[5] http://www.qi.mp.es.osaka-u.ac.jp/

4. *Hai-Woong Lee, S.M.Lee*
(KAIST, Daejeon, Korea)
Proposal for Experimental Schemes to Measure Entanglement

One of the key issues in quantum information science is how to detect and measure entanglement. In this talk we describe experimental schemes to measure the amount of entanglement of a two-qubit (or, in general, two-qudit) system.

We first describe a cavity-qed scheme of directly measuring the concurrence of a two-qubit cavity system. The scheme derives from the realization that the concurrence coincides with the two-particle visibility under suitable interferometer setups. It requires standard cavity field-atom interactions, dispersive interactions and Ramsey zones, and can be realized within present cavity qed technologies. The scheme works for any arbitrary pure state of a two-qubit cavity system.

The above scheme and other schemes proposed in the past to measure entanglement typically require measurements to be performed on the entire composite system and involve coincidence measurements and/or complex controlled operations. On the other hand, it is possible to measure entanglement by performing measurements on one of the subsystems only, owing to the complementarity relation between the amount of entanglement and the purity of a subsystem. We propose a simple method of measuring the purity of a pure state of a subsystem of any arbitrary dimension. It requires only single qudit rotations and straightforward probability measurements and can thus be easily implemented experimentally using linear optical devices. The number of required experimental setups scales linearly with the dimension of the subsystem being measured.

5. *Serge Massar*
(University of Brussels, Brussels, Belgium)
Secret keys and random numbers based on quantum non locality

We discuss how non local correlations shared by two parties can be used to generate a secret key. We also discuss how non local correlations can be used to generate random numbers. Using non locality allows a higher degree of security than in the more traditional approaches, indeed it is no longer necessary to trust one's devices, nor even to trust quantum mechanics.

6. *Karol Życzkowski, P.Gawron, Z.Puchała, J.A.Miszczak, Ł.Skowronek and M.D.Choi*
(Jagelonian University, Cracow, Poland)
Local numerical range: a versatile tool in the theory of quantum information

We study operators acting on a composite Hilbert space and investigate their local numerical range, local spectral radius and local C–spectral radius. For any Hermitian operator X acting on a bi-partite Hilbert space its local numerical range is formed by the set of all possible expectation values of X among pure product states, $\langle \phi \otimes \psi | X | \phi \otimes \psi \rangle$. Concrete bounds for the local numerical range for Hermitian operators are derived.

Local numerical range of a non-Hermitian operator forms a subset of the standard numerical range. While the latter set is convex, the local range needs not to be convex nor simply connected. Local numerical range of a tensor product is equal to the Minkowski product of numerical ranges of individual factors.

As an exemplary application of these algebraic tools in the theory of quantum information we study block positive matrices and entanglement witnesses. Furthermore, we apply local numerical range to solve the problem of local distinguishability of a family of two unitary gates. Local C–spectral radius is useful for finding local fidelity between two states of a composite system, while higher order local numerical range can be used to design local dark spaces and local error correction codes.

CONTRIBUTED TALKS

1. *Jan Bouda, J.Miszczak und M.Ziman*
(Masaryk University, Brno, Czech Republic)
Private quantum channels, multi-photon pulses and unitary k-designs
Private quantum channel is a formalism of encryption of quantum information. Encryption is realized via application of a unitary operator chosen randomly from a pre-designed public set U_{ii} according to a publicly known probability distribution p_i to the plaintext state ρ. The security criterion reads that there is a fixed state $\rho^{(0)}$ such that for every plaintext state ρ it holds that

$$\sum_i p_i U_i \rho U_i^\dagger = \rho^{(0)}.$$

In case of experimental realization we are facing the problem of multi-photon pulses, i.e. instead of a single photon a k-photon pulse is sent through the encryption device. This, in fact, is equivalent (depending on the experimental setup) to the situation when we send k copies of the plaintext state and encrypt each copy using the same unitary operation. The average output in this case reads

$$\sum_i p_i U_i^{\otimes k} \rho^{\otimes k} {U_i^\dagger}^{\otimes k},$$

what is in general dependent on ρ.

In our talk we focus on the problem whether we can design a specific private quantum channel, i.e. the set of operators $\{U_i\}_i$ together with a suitable probability distribution, such that the aforementioned expression is independent of ρ. We show that this is impossible provided ρ ranges though all quantum (mixed!) states. On contrary, it becomes possible when ρ can be only a pure state and the solution for at most k-photon pulse is any unitary k-design.

2. *Miloslav Dušek, L.Bartušková, M.Mičuda, J.Fiurášek, M.Ježek, A. Černoch, J.Soubusta*
(Department of Optics, Palacky University, Olomouc, Czech Republic
Linear-optical quantum information processing - a few experiments
Quantum information processing requires precise manipulation and measurement of the states of quantum systems. Even if linear-optical implementations of quantum operations are mostly probabilistic, they have a big potential for practical realization of many quantum information processing tasks. In this contribution we review some our recent experiments in this field. Namely, linear-optical implementations of a Programmable discriminator of unknown non-orthogonal polarization states of a photon, an Encoder of two qubits into a single qutrit, a Programmable discriminator of weak coherent states, Partial-SWAP gates including entangling square-root of SWAP, and a Programmable gate for an arbitrary rotation of a single qubit along the z axis. Some of these experiments were built from bulk optical elements and the information was encoded into polarization states of photons. The others were based on fiber optics. In these cases the information was encoded into spatial modes, i.e. each photon could propagate through two or more optical fibers.

3. *Ivan Fialík*
(Masaryk University, Brno, Czech Republic)
Cryptographic Applications of Pseudo-Telepathy Games
A pseudo-telepathy game is a cooperative game for two or more players for which there is no classical winning strategy, but there is a winning strategy based on sharing quantum entanglement by the players. After introducing a model for pseudo-telepathy games, we focus on cryptographic applications of these games. We propose simple protocols for user identification and data authentication in which the parties play some pseudo-telepathy game using their shared entangled quantum state. We also investigate the suitability of several known pseudo-telepathy games for cryptographic purposes in the sense of security properties of the resulting protocols.

4. *Zeynep Nilhan Gurkan, O.K. Pashaev*
(Izmir Institute of Technology, Turkey)
Entanglement Evolution for Anisotropic Heisenberg Models with DM Interaction
System of two qubits, interacting by Heisenberg XYZ anisotropic and Dzialoshinskii-Moriya (DM) antisymmetric exchange interaction models are considered. The Von Neumann entropy and the concurrence measurement of the entanglement are calculated and compared. The entanglement evolution is calculated by using the evolution operator. It is shown that for specific choice of parameters entanglement is a periodic function of external parameters, the exchange integrals and the DM coupling. By analytic continuation of the evolution to the Euclidean time we find corresponding density operator and calculate the thermal entanglement and dependence on the temperature. It is shown that evolution of entanglement in the Euclidean time has dissipative form and in all cases could be enhanced by the DM coupling parameter.

5. *Min-Hsiu Hsieh and M.M.Wilde*
(ERATO-SORST, Tokyo, Japan)
Public and private communication with a quantum channel and a secret key
We consider using a secret key and a noisy quantum channel to generate noiseless public communication and noiseless private communication. The optimal protocol for this setting is the publicly-enhanced private father protocol. This protocol exploits random coding techniques and p̈iggybackingöf public information along with secret-key-assisted private codes. The publicly-enhanced private father protocol is a generalization of the secret-key-assisted protocol of Hsieh, Luo, and Brun and a generalization of a protocol for simultaneous communication of public and private information suggested by Devetak and Shor.

6. *Marcus Huber, B.Hiesmayr*
(University of Wien, Wien, Austria)
Multipartite entanglement measures
We present two sets of computable measures for multipartite system of discrete subsystems. Bounds on both measures can be computed by discovering that any entropy can be rewritten via a quantity called m–concurrence and on these quantities one can operationally obtain bounds via a convex roof construction. We show for many examples, e.g. GHZ, W state, generalized Smolin state, generalized Werner states,dots that often the bounds are tight and show that in general they involve even for multipartite qudits only the computation of $d = 4$ matrices, making it a feasible method for complex systems.

7. *Piotr Kolenderski, R.Demkowicz-Dobrzanski*
(Nicolaus Copernicus University, Torun, Poland)
Alignment of reference frames and platonic solids
The two most commonly used physical systems for the reference frames alignment are: the system of N distinguishable qubits and the system of N qubits in a fully symmetric state. The former are physically equivalent to N spins $1/2$ or polarization states of N photons traveling in separate time-bins and the last to bosonic states, e.g. polarization states of photons traveling in a single time-bin. Much work has been done within the global approach, namely when there is no initial information about reference frame. The optimal states are known for phase, direction and cartesian frame encodings, both when using N distinguishable qubits and when using them in a fully symmetric state or equivalently using a single spin $J = N/2$, see Ref. [1] and references therein.

This paper [2] fills the missing gap by presenting the optimal state for reference frame alignment within the local approach, when two parties possess some information about the initial orientation and their goal is to measure a small misalignment. The optimal N qubit states featuring highest sensitivity to small misalignment of cartesian reference frames are found using the Quantum Cramér-Rao bound. It is shown that the optimal states are supported on the symmetric subspace and hence are mathematically equivalent to a single spin $J = N/2$. We prove that in the local approach distinguishability of the qubits gives no advantage over the use of N qubits in the fully symmetric state or a single spin $J = N/2$ – a fact known for phase and direction reference alignment.

Moreover the Majorana representation [3] of spin states is used to reveal a beautiful connection between the states optimal for aligning reference frames and the platonic solids. For example the simplest optimal states of $N = 4$ and $N = 6$ qubits correspond to the tetrahedron and octahedron, respectively. The intuitions gained within the Majorana representation allowed to find the classes of optimal states for higher number N of spins corresponding to each platonic solid.

[1] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. 79, 555 (2007).
[2] P. Kolenderski and R. Demkowicz-Dobrzanski, Phys. Rev. A 78, 052333 (2008).
[3] E. Majorana, Nuovo Cimento 9, 43 (1932).

8. *Cosmo Lupo, V.Giovannetti, S.Mancini*
(University of Camerino, Camerino, Italy)
Capacities of lossy bosonic memory channels
We introduce a general model for a lossy bosonic memory channel and calculate the classical and the quantum capacity, proving that coherent state encoding is optimal. The use of a proper set of collective field variables allows to unravel the memory, showing that the n-fold concatenation of the memory channel is unitarily equivalent to the direct product of n single-mode lossy bosonic channels.

9. *Daniel Nagaj, P.Wocjan, Y.Zhang*
(Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia)
Fast QMA amplification
Given a verifier circuit for a problem in QMA, we show how to exponentially amplify the gap between its acceptance probabilities in the "yes" and "no" cases, with a method that is

quadratically faster than the procedure given by Marriott and Watrous. Our construction is natively quantum, based on the analogy of a product of two reflections and a quantum walk. Second, in some special cases we show how to amplify the acceptance probability for good witnesses to 1, making a step towards understanding the relationship of QMA and QMA with one-sided error. Finally, we simplify the filter-state method to search for QMA witnesses by Poulin and Wocjan.

10. *P. Rapčan, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, and V. Bužek*
(RCQI, Bratislava, Slovakia)
Recycling of Quantum Information
It is well known that there exists an "information-disturbance" tradeoff between the quality of estimating a state of a quantum system and the degree the initial state has to be altered in the course of the estimation procedure carried by an observer. This means the after-measurement state can still carry partial information on the initial quantum state which can be estimated by further observer whose estimation procedure (in general) again introduces further disturbance and so on. Consequently, one can pose several questions related to the estimation fidelity of the kth observer under reasonable assumptions under which the answers to these questions are not trivial, which is what we do.

To be specific, we consider the following situation: a pure state of a d-dimensional system known to the preparer but unknown to the observers is encoded into a pure state (from a $SU(d)$-invariant family of states) of a D-dimensional system. The encoding is $SU(d)$-covariant. The preparer or any of the observers do not share a basis (nor a set of bases other than the whole set $\{U|0\rangle,\ U \in SU(d)\}$) nor do they possess or communicate any information that would reveal (or constrain the possible set of) their estimation results, not even probabilistically. Each observer uses an estimation strategy introducing minimal disturbance given an information gain. We calculate the maximum average estimation fidelity for the kth observer if: i) each observer's strategy maximizes his estimation fidelity; ii) each of the observers' strategies maximize their estimation fidelities given the condition that all observers' fidelities have to be the same (each observer knows his order, k); iii) each of the observers' strategies maximize the fidelity of the last observer's estimation given the condition that all observers' strategies (i.e. quantum instruments) have to be the same. The total number of observers, K, is fixed and known to the observers in the cases ii) and iii). We solve the problems i): for any $d = D$, for any $2 = d < D$, and for any $2 = d < D$ with the restriction of encoding into copies; ii) and iii): for any $d = D$ and for any $2 = d < D$ with the restriction of encoding into copies (leading orders asymptotically, $K \gg D$ and $D \ll K$).

11. *Daniel Reitzner, M.Hillery, E.Feldman, and V.Bužek*
(Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia)
Quantum searches on highly symmetric graphs
We show how to apply scattering quantum walks on highly symmetric graphs to solve search problems on these graphs for one of the marked target vertices. Scattering properties of the vertices depend on whether they are the target ones or not. To provide such differentiation we employ a quantum circuit that utilizes standard Grover oracle alongside presented evolution of the walk. This circuit allows us to separate oracular elements of the problem from the rest of the evolution. As graphs we consider complete graph, complete bipartite graph, and an M-partite graph as their common generalization. In all considered graphs, for the symmetry

reasons — these graphs have large automorphism groups — the evolution takes place in a Hilbert space of small dimension, not unlike in standard Grover search.

12. *Wojciech Roga, M.Fannes, K.Życzkowski*
(Jagiellonian University, Krakow, Poland)
One qubit maps compatible with the interaction with an environment
A model system of one qubit interacting with a multipartite environment in a thermal equilibrium is analysed. We consider a class of one-qubit maps which are compatible with the interaction with the environment in the sense that they preserve the equilibrium state. A full describtion of these completely positive and trace preserving maps, which satisfy this condition is provided. We discuss also a possible generalization of these results for three level systems.

13. *Michal Sedlák, M.Ziman*
(Institute of Physics, Bratislava, Slovakia)
Unambiguous comparison of unitary channels
We shall investigate the problem of an unambiguous comparison of a pair of unknown qudit unitary channels [1]. Using the framework of process positive operator valued measures (PPOVM) [2] we characterize all solutions and identify the optimal ones. We prove that the entanglement is the key ingredient in designing the optimal experiment for comparison of unitary channels. Without the entanglement the optimality cannot be achieved.

[1] M.Sedlak, M.Ziman, Phys.Rev.A 79, 012303 (2009) [arXiv:0809.4401]
[2] M.Ziman, Phys.Rev.A 77, 062112 (2008) [arXiv:0802.3862]

14. *Jan Vlach, T.Tyc*
(Masaryk University, Brno, Czech Republic)
Gaussian quantum marginal problem
We look for relations between the global symplectic spectrum of the whole system and local symplectic spectra of its k-mode subsystems. The solution is known for k = 1, but I would like to introduce some conjectures for more general cases.

POSTERS

1. *Wojciech Bruzda, M.Smaczyński, K.Życzkowski*
(Jagiellonian University, Kraków, Poland)
Spectral gap and convergence to invariant state in open quantum systems
We investigate typical quantum operators, describing evolution of an open quantum system, for which there exist a unique invariant state ω. The relaxation time at which any initial state converges to ω is governed by the spectral gap of the corresponding superoperator. The size of the spectral gap is studied for a class of modified quantum baker maps and compared with the properties of a random quantum system.

2. *Mátyás Koniorczyk, P. Rapčan, A. Varga and V. Bužek*
(Institute of Physics, University of Pécs, Hungary)
State randomization and quantum homogenization in semi-quantal spin systems
We investigate dynamics of semiquantal spin systems in which quantum bits are attached to classically and possibly stochastically moving classical particles. The interaction between

the quantum bits takes place when the respective classical particles get close to each other in space. We find that with Heisenberg XX couplings quantum homogenization takes place after a long enough time, regardless of the details of the underlying classical dynamics. This is accompanied by the development of a stationary bipartite entanglement. If the information on the details of the motion of a stochastic classical system is disregarded, the stationary state of the whole quantum subsystem is found to be a complete mixture in the studied cases, though the transients depend on the properties of the classical motion.

3. *Katalin Hangos, G. Ballo, A. Magyar*
(Computer and Automation Research Institute, Budapest, Hungary)
Optimal quantum process tomography and experiment design for single parameter quantum channels
A quantum process tomography problem is solved in this work together with an optimal POVM selection. Both the process tomography and the experiment design are solved numerically as convex optimization problems. The quantum channel is an arbitrary one, parameterized by a single scalar parameter. The optimal POVM is a convex combination of von Neumann projections, and the optimizing variables of the experiment design problem are the coefficients of these projections. To find the optimal measurement, one has to solve a constrained convex optimization problem, using the norm of the difference between classical Fisher information and the quantum Helstrom information as objective function. This is based on the inequality stating that the Helstrom information is an upper bound for the Fisher information. Both tomography and POVM optimization is solved in Matlab/SDPT3 environment.

4. *Martin Plesch, V.Bužek*
(RCQI, Bratislava, Slovakia)
Efficient compression of unknown quantum information
We propose a scheme for efficient transformation of a tensor product state of many identical qubits into a state of exponentially small number of qubits. By a quadratic number of elementary quantum gates we rewrite N copies of one qubit (spanned on $O(2^N)$ computational state vectors) into a state, which is nontrivial only on first $log(N)$ qubits. Such a procedure might be very useful for quantum memories or for sending of a direction encoded in a set of quantum states.

5. *Nikolajs Nahimovs, Alexander Rivosh* (University of Latvia, Latvia)
Grover algorithm with probabilistic solutions
In our poster, we study two modifications of Grover algorithm. First, we consider a Grover algorithm where solutions are probabilistic. That is, with certain probability query transformation is omited or replaced with another transformation. Secondly, we consider a Grover algorithm with probabilistic "fake" solutions. That is, we study the behavior of Grover algorithm when with a certain probability an extra transformation is applied after a query.

6. *Dmitry Kravchenko*
(University of Latvia, Latvia)
Non-locality and quantum games
Quantum non-local games introduce one of the most counterintuitive phenomena of quantum mechanics. Thus, use of two entangled qubits in the CHSH game allows to achieve

significantly higher probability of winning. This famous game demonstrates provably best improvement in two players games, which could be reached with quantum mechanical effects. In the poster, we will study some interesting aspects of non-local games, consider some important limitations for them, and find the ways for the further quantum improving of strategy in such games. As a part of the poster, IÍl describe at least one four players game, for which quantum strategy gives higher improvement than for any two players game.

7. *Iman Marvian*
(IQC, University of Waterloo, Canada)
Simulating all time evolutions with rotationally invariant Hamiltonians and quantum reference frames
It sometimes occurs that the only unitary time evolutions that can be achieved on a system are those that are rotationally invariant. This restriction may arise from practical issues such as two distant parties lacking a shared directional reference frame. It may also be a consequence of the symmetries of fundamental interactions in nature. This restriction can be overcome, however, by using a quantum reference frame which allows one to simulate time evolutions which are not rotationally invariant. In this work we demonstrate that with the use of a sufficiently large reference frame one can always simulate any given non-invariant Hamiltonian or any given non-invariant unitary time evolution with arbitrary precision. We compare schemes that differ in the state of the quantum reference frame. We also discuss how the quality of the simulation depends on the size of the reference frame.

8. *Miroslava Sotáková, L.Salvail, C.Schaffner*
(Bratislava, Slovakia)
On the power of two-party quantum cryptography
We study quantum protocols among two distrustful parties. Under the sole assumption of correctness - guaranteeing that honest players obtain their correct outcomes, we show that every protocol implementing a non-trivial primitive necessarily leaks information to a dishonest player. This extends known impossibility results to all non-trivial primitives. We provide a framework for quantifying this leakage and argue that leakage is a good measure for the privacy of a given protocol. All our results hold even against quantum honest-but-curious adversaries who honestly follow the protocol but purify their actions and apply a different measurement at the end of the protocol. As concrete examples, we establish lower bounds on the leakage of standard universal two-party primitive such as oblivious transfer. Furthermore, we also discuss composability of two-party quantum protocols.

Lecture Hall

Hotel
Na 15. poledníku

Hotel
Černej pták

Hotel
Concertino

Hotel
Bílá paní

Rondel

List of participants

1. Jan Bouda (Brno, Czech Republic)
2. Wojciech Bruzda (Cracow, Poland)
3. Vladimír Bužek (Bratislava, Slovakia & Brno, Czech Republic)
4. Libor Caha (Brno, Czech Republic)
5. Giacomo Mauro D'Ariano (Pavia, Italy)
6. Miloslav Dušek (Olomouc, Czech Republic)
7. Jens Eisert (Potsdam, Germany)
8. Ivan Fialík (Brno, Czech Republic)
9. Jozef Gruska (Brno, Czech Republic)
10. Zelnep Nilhan Gurkan (Izmir, Turkey)
11. Katalin Hangos (Budapest, Hungary)
12. Marcus Huber (Wien, Austria)
13. Min-Hsiu Hsieh (Tokyo, Japan)
14. Nobuyuki Imoto (Osaka, Japan)
15. Piotr Kolenderski (Torun, Poland)
16. Mátyás Koniorczyk (Pecs, Hungary)
17. Dmitry Kravchenko (Riga, Latvia)
18. Hai-Woong Lee (Daejeon, Korea)
19. Cosmo Lupo (Camerino, Italy)
20. Iman Marvian (Waterloo, Canada)
21. Serge Massar (Brussels, Belgium)
22. Daniel Nagaj (Bratislava, Slovakia)
23. Nikolajs Nahimovs (Riga, Latvia)
24. Michael Nölle (Seibersdorf, Austria)
25. Denes Petz (Budapest, Hungary)
26. Matej Pivoluška (Brno, Czech Republic)
27. Martin Plesch (Bratislava, Slovakia)
28. Peter Rapčan (Bratislava, Slovakia)
29. Daniel Reitzner (Bratislava, Slovakia)
30. Alexander Rivosh (Riga, Latvia)
31. Wojciech Roga (Cracow, Poland)
32. László Ruppert (Budapest, Hungary)
33. Michal Sedlák (Bratislava, Slovakia)
34. Miroslava Sotáková (Bratislava, Slovakia)
35. Levente Szabó (Pecs, Hungary)
36. Jan Vlach (Brno, Czech Republic)
37. Mário Ziman (Bratislava, Slovakia & Brno, Czech Republic)
38. Karol Życzkowski (Cracow, Poland)

CONFERENCE PROGRAM

Monday, 1.6.2009

17:00 Afternoon session (chaired by Vladimír Bužek)
17:00 J. Eisert: Too entangled to be useful?
17:45 break
17:55 G.M. D'Ariano: The quantum comb: theory and applications to quantum networks
18:55 End of session
19:00 Bier & Barbeque Dinner Party (Hotel Concertino)

Tuesday, 2.6.2009

09:00 Morning session (chaired by Giacomo Mauro D'Ariano and Denés Petz)
09:00 N.Imoto: Backaction control in quantum measurement ...
09:45 M.Dušek: Linear-optical quantum information processing - a few experiments
10:05 M.Sedlák: Unambiguous comparison of unitary channels
10:25 Coffee break
10:55 H.W. Lee: Proposal for experimental scheme to measure entanglement
11:40 M. Huber: Multi-partite entanglement measures
12:00 Lunch
15:00 Afternoon session (chaired by Matyás Koniorczyk)
15:00 D. Nagaj: Fast QMA amplification
15:20 D. Reitzner: Quantum searches on highly symmetric graphs
15:40 Coffee break
16:00 Poster session
19:00 Social dinner

Wednesday, 3.6.2009

09:00 Morning session (chaired by Miloslav Dušek and Mário Ziman)
09:00 S. Massar: Secret keys and random numbers based on quantum nonlocality
09:45 M.H. Hsieh: Public and private communication with a quantum channel and a secret key
10:05 W. Roga: One qubit maps compatible with the interaction with an environment
10:25 Coffee break
10:55 J. Bouda: Private quantum channels, multi-photon pulses and unitary k-designs
11:15 I. Fialík: Cryptographic applications of pseudo-telepathic games
11:35 P. Rapčan: Recycling of quantum information
12:00 Lunch
15:00 Castle sightseeing (details later)
19:00 Conference dinner (Rondel, castle)

Thursday, 4.6.2009

09:00 Morning session (chaired by Jozef Gruska)
09:00 K. Życzkowski: Local numerical range: a versatile tool in the theory of quantum information
09:45 P. Kolenderski: Alignment of reference frames and platonic solids
10:05 Coffee break
10:45 C. Lupo: Capacities of lossy bosonic channels
11:00 J. Vlach: Gaussian quantum marginal problem
11:15 Z.N. Gurkan: Entanglement evolution for anisotropic Heisenberg models with ...
11:45 Lunch