

Quantum Technologies in Czechia Roadmap

May 29, 2017

Contents

Multi-photon sources of light	2
Quantum state engineering and detection for quantum metrology and sensing	2
Quantum tomography, estimation and enhanced super-resolution	3
Multi-photon quantum optics for quantum communications	4
Quantum key distribution	5
Sensing of non-classical light and diagnostics of matter	5
Sensing and manipulation of quantum motion	6
Analog quantum non-linear gates	7
Optical frequency metrology and spectroscopy with laser cooled ions	7
Quantum physics with levitating objects	8
Quantum networks	9
Quantum walks	10
Nonlinear optical networks	10
Quantum nanophotonics and nanoplasmonics	11
Quantum sensing and imaging using color centers in diamond	12
Self-assembled layers of molecular qubits with tunable spin interactions	13
Quantum computation and simulation in chemistry	13
Quantum information theory and quantum cryptography	14
Quantum and classical communication complexity	15
Quantum computing of statistical physics phenomena	15

Multi-photon sources of light

Pillars: Quantum Communication, Quantum Metrology and Sensing, Enabling Science

Contact person: Radim Filip, filip@optics.upol.cz

Institutions: Department of Optics, Faculty of Science, Palacký University, Olomouc

Know how: We have a long-term experience with developing sources of non-classical multi-photon states based on nonlinear processes in matter. It is complemented by long-term expertise in photo-detection techniques useful for applications in quantum communication and quantum metrology. We have also unique skills in developing quantum protection techniques for shielding multi-photon states against environmental decoherence. In this subject, we participated in international consortia supported by the EU Framework Projects (including the last FP7).

Research goals: We plan to apply our knowledge to the generation of optimal multi-photon states for short-range optical connections of quantum devices and for efficient and robust optical control and readout in quantum metrology.

Excellence, Uniqueness: We have a unique experience in proposing feasible schemes for generation and manipulation of multi-photon states of light and long-term high-quality international collaboration focused on their proof-of-principle tests.

Benefit for Czechia: This direction allows access to modern technology of multi-photon state generation and detection. In the future, this will be an appropriate topic for applied research.

Quantum state engineering and detection for quantum metrology and sensing

Pillar: Quantum Metrology and Sensing, Enabling Science

Contact person: Jan Peřina, jr., jan.perina.jr@upol.cz

Institution: Joint Laboratory of Optics of Palacký University and Institute of Physics of Czech Academy of Sciences, Olomouc

Know how: Long lasting experience with building of photon-number-resolving detectors (time and spatial multiplexed counting devices, iCCD cameras) and their applications in the analysis of entangled twin beams composed of many photon pairs. We have measured joint signal-idler photo-count distributions and reconstructed the analyzed twin beams, developed a method for absolute detector calibration, studied entanglement in a twin beam as well analyzed spatial correlations in the twin beam. We have also employed the spatial, spectral and photon-number correlations in twin beams to produce highly non-classical multi-photon states of light.

Research goals: Our research is primarily focused on the photo-count measurements of twin beams, preparation of special states using a twin beam (e.g. sub-Poissonian light via post-selection), analysis of quantum correlations in such states. We plan to widen these investigations, namely those of entanglement in twin beams and more complex states emerging in nonlinear interaction with the aim to demonstrate their usefulness for the implementation of various precise metrological methods and also quantum-information protocols.

Excellence, Uniqueness: Our research is based on special reconstruction methods for revealing the states of entangled quantum fields composed of a larger number of correlated photons (photon-pairs) that were developed during the last 15 years. They extensively use iCCD cameras that are practical for photon counting. The method enables to study quantum correlations in more complex Hilbert spaces spanned by the Fock states with larger photon numbers which makes it promising for future metrology methods as well as quantum-information processing. Also, spatial and spectral correlations in a twin beam largely experimentally analyzed in the past represent an important part of our unique knowledge.

Benefit for Czechia: New metrology techniques will be developed that can bring new level of precision or enlarge the field of applicability. Quantum-information protocols will be applied to more complex Hilbert spaces, thus enriching the quickly growing field of quantum communications and quantum information processing. Last but not least, students will be educated in novel methods of detection and analysis of photon fields.

Quantum tomography, estimation and enhanced super-resolution

Pillar: Quantum metrology and sensing, Enabling Science

Contact person: Zdeněk Hradil, hradil@optics.upol.cz

Institutions:

- Department of Optics, Faculty of Science, Palacký University, Olomouc
- Institute of Scientific Instruments of the Czech Academy of Sciences, Brno

Know how: There is a substantial know-how systematically accumulated during last twenty years. The research has started in the framework of neutron optics and quantum interferometry in 1990s and later on has been spread into quantum tomography. MaxLik tomography and other reconstruction methods are used nowadays as a standard tool. Current research is oriented on the advanced detection methods in optics such as Shack-Hartmann detection, and on the problems of super-resolution related to the concept of quantum Fisher information.

Research goals: The goal of the program is to push the performance of existing optical detection techniques up to their fundamental limits as far as precision and range of parameters is concerned. The advanced detection techniques will fully exploit the potential of detection and modulation of faint signals.

Excellence, Uniqueness: The research is based on the current state of the art in optical technology. The understanding (and possible achieving) of ultimate limits is of paramount importance for other branches of sciences hinging upon optical detection techniques. Such techniques even with classical signals but inspired by quantum technologies are close to real applications.

Benefit for Czechia: Optical research and industry has long and successful tradition in Czech. Our new techniques with classical signals inspired by quantum theory are probably the closest to real-live applications.

Multi-photon quantum optics for quantum communications

Pillar: Quantum Communication, Enabling Science

Contact person: Karel Lemr, k.lemr@upol.cz

Institution: Joint Laboratory of Optics of Palacký University and Institute of Physics of Czech Academy of Sciences, Olomouc

Know how: Since the 90s, our lab has been focused on the field of quantum communications, namely on quantum cryptography and subsequently also on quantum cloning as a means of cryptography attack. This research was followed by a wider class of two-photon quantum gates (e.g. SWAP or CNOT gate). Recently, we have increased the portfolio of our research techniques by developing three and four-photon sources. Using these sources, we are currently investigating two related aspects of quantum communications: (i) practical techniques for entanglement detection and (ii) advanced linear-optical active elements for quantum networks.

Research goals: Our research involves quantum-optical experiments with multiple photons and related theoretical work. The aim is to perform fundamental research with application potential for future quantum communications networks. We plan on constructing complex linear-optical setups implementing crucial protocols allowing quantum networks to increase their complexity (quantum routers) as well as the attainable distances (amplifiers).

Excellence, Uniqueness: The capability to manipulate up to four discrete photons simultaneously gives us an opportunity to perform state-of-the-art experiments in the field of quantum optics. Moreover, our research combines fundamental topics (e.g. entanglement detection using non-linear witnesses) with development of crucial protocols for complex quantum communications networks (e.g. quantum routers). As an example, we have recently proposed and tested an efficient entanglement detection protocol operating in the geometry of entanglement-swapping devices which can be straightforwardly used for diagnostics of quantum repeaters.

Benefit for Czechia: Since quantum communications represent a significant potential for secure communications, having national research in this field can improve cybersecurity of our country. Additionally, students will be trained in both theoretical background and experimental

techniques of quantum communications giving them exclusive place on the job market both nationally and worldwide.

Quantum key distribution

Pillar: Quantum Communication

Contact persons:

- Radim Filip, filip@optics.upol.cz
- Miloslav Dušek, dusek@optics.upol.cz

Institutions:

- Department of Optics, Faculty of Science, Palacký University, Olomouc
- CESNET, z. s. p. o., Praha

Know how: Already in 1997 we built a laboratory prototype of a fully functional device for quantum key distribution and mutual identification. We had also participated in the large European integrated project SECOQC and we are involved in the SPACE-QUEST initiative. We have experience with development of quantum key distribution protocols exploiting multi-photon states of light and high-speed detection, as well as with security analysis of quantum key distribution under realistic assumptions for free-space and fiber-based channels.

Research goals: We will focus on development of quantum key distribution with multi-photon states in already existing small fiber networks, short-distance free-space channels and its possible extension to space. We will also analyze security of practical QKD devices with side-channels.

Excellence, Uniqueness: We have a unique experience in the feasibility study of quantum key distribution with multi-photon non-classical states and high-speed detection and analysis of its applicability in realistic conditions. We have a long-term experience in quantum cryptography research.

Benefit for Czechia: We have direct access to modern quantum communication technology and international collaboration with the leading teams in quantum cryptography. It is already an appropriate subject for transfer between basic and applied research.

Sensing of non-classical light and diagnostics of matter

Pillars: Quantum Metrology and Sensing, Enabling Science

Contact person: Radim Filip, filip@optics.upol.cz

Institutions:

- Department of Optics, Faculty of Science, Palacký University, Olomouc
- Institute of Scientific Instruments of the Czech Academy of Sciences, Brno

Know how: We have successfully developed detection techniques, data processing, and criteria for sensing of non-classical light emitted by matter (like optical structures, atoms and solid state systems). We have also a long-term experience with identification and modeling of fundamental processes in quantum matter. We have experimentally verified new features of highly nonclassical light from optical and atomic structures.

Research goals: Diagnostics of the states of matter by analyzing a hierarchy of non-classical properties of the emitted light. This will deepen the understanding of truly quantum processes undergoing in atoms, molecules and solid-state structures.

Excellence, Uniqueness: We have a long-term unique expertise in development of feasible operational criteria enabling us to detect non-classical states of light. At the same time, we have long-term knowledge in their experimental exploitation.

Benefit for Czechia: This direction enables the fundamental study of matter states and offers broad access to modern detection and sensing technologies operating at the quantum level. In the future, it will be an appropriate topic for applied research.

Sensing and manipulation of quantum motion

Pillars: Quantum Metrology and Sensing, Enabling Science

Contact person: Radim Filip, filip@optics.upol.cz

Institutions:

- Department of Optics, Faculty of Science, Palacký University, Olomouc
- Institute of Scientific Instruments of the Czech Academy of Sciences, Brno

Know how: We have developed quantum detection and manipulation methods for optomechanical systems (membranes, cantilivers, nanostructures, nanoparticles, trapped ions) operating in the pulsed regime. We have shown how they can be exploited in quantum metrology of motion. This research is currently expanding under the cover of the undergoing Center of Excellence of the Czech Science Foundation.

Research goals: We will exploit non-classical states of motion and non-classical states of light to improve quantum sensors. We will apply pulsed quantum interfaces and transducers accessing different experimental platforms to broader access of these quantum sensors.

Excellence, Uniqueness: We have a deep and unique knowledge of pulsed quantum opto-mechanics and electro-mechanics together with long-term experience in applications of non-classical light. We already have a unique ability to experimentally test it using trapped ions and in future we will expand this ability to trapped nanoparticles.

Benefit for Czechia: We experimentally develop quantum metrology of motion with trapped ions and nanoparticles in Czechia. We provide direct access to modern technology of quantum opto-mechanics and its applications in metrology and mechanical manipulations. In the future, it will be an appropriate topic for applied research.

Analog quantum non-linear gates

Pillars: Quantum Simulation, Quantum Computation, Enabling Science

Contact person: Radim Filip, filip@optics.upol.cz

Institutions:

- Department of Optics, Faculty of Science, Palacký University, Olomouc
- Institute of Scientific Instruments of the Czech Academy of Sciences, Brno

Know how: We have a long-term and broad experience with theoretical development of nonlinear quantum gates with optical, electrical, and mechanical oscillators, including their applications in analog quantum simulators with complex oscillators. We have a deep knowledge of the analysis of quantum dynamics of nonlinear oscillators as well as the ideas for potential applications. Developing quantum nonlinear physics with trapped ions and nanoparticles is the main subject of the currently running joint Center of Excellence.

Research goals: We plan to develop an analog quantum simulator capable of simulating unexplored nonlinear effects in open systems and test its application in quantum thermodynamics.

Excellence, Uniqueness: We are able to uniquely analyze mechanical systems operating in quantum regime with strong non-linearity and high-quality optical control. We are able to test quantum mechanical nonlinear effects with the trapped ions.

Benefit for Czechia: We have a potential to experimentally develop analog quantum simulators in the Czech Republic in the collaboration with leading foreign groups.

Optical frequency metrology and spectroscopy with laser cooled ions

Pillars: Quantum Metrology and Sensing, Enabling Science

Contact persons:

- Ondřej Číp, ocip@isibrno.cz
- Josef Lazar, joe@isibrno.cz
- Lukáš Slodička, slodicka@optics.upol.cz
- Josef Vojtěch, josef.vojtech@cesnet.cz

Institutions:

- Institute of Scientific Instruments of the Czech Academy of Sciences, Brno
- Department of Optics, Faculty of Science, Palacký University, Olomouc
- CESNET, z. s. p. o., Praha

Know how: Theoretical and experimental knowledge in the area of optical frequency standards and sensors based on the laser oscillators disciplined with quantum states of trapped ions (Ca^+). We participate also on a joint effort with the national metrology authority and providers of long-haul fibre optic links directed to the distribution of highly stable optical frequencies over distances at hundreds kilometers.

Research goals: Our activities are now focused on the finalizing the experimental setup where the clock laser will be locked to the forbidden transition of Ca^+ ions and spectroscopy behaviors of the cooled ion are analyzed with respect to its motional state. We further plan to build-up the research infrastructure for motional manipulations of single ions confined in a novel segmented Paul trap with the focus on the possibility of effective design of nonlinear potentials and tunable motional coupling between neighbouring ions.

Excellence, Uniqueness: Our research has very promising link to application in molecular spectroscopy based conventional optical frequency standards. In this field the ultimate stability clock lasers Ca^+ can be used for minimizing of some parts of the uncertainty budget of these conventional standards. The laser cooled ions are also very promising single photon sources for the quantum metrology which helps to improve the resolution of measuring methods in the length and frequency metrology.

Benefit for Czechia: The unique quantum based infrastructure will be created which provides the fundamental research in the branch of quantum sensors and quantum simulators with practical outcomes in the length or frequency metrology, new industrial emerging technologies (in automotive, optics and ICT) and the environmental sensing (geological and space survey).

Quantum physics with levitating objects

Pillars: Quantum Metrology and Sensing, Enabling Science

Contact person: Pavel Zemánek, zemanek@isibrno.cz

Institutions:

- Institute of Scientific Instruments of the Czech Academy of Sciences, Brno
- Department of Optics, Faculty of Science, Palacký University, Olomouc

Know how: Theoretical and experimental knowledge in the area of optical micro-manipulation techniques with nano-objects or micro-objects has been developing since 1995.

Research goals: The activities are now focused on the optical levitation and cooling of mechanical degrees of freedom of nano-objects in an ambient with extremely low damping.

Excellence, Uniqueness: An optically confined object represents a high quality mechanical oscillator with very low damping having orders of magnitude higher sensitivity for mechanical force and torque detection. Even though the mechanical quantum state of the object has not been reached yet worldwide, this direction is considered as one of the promising candidates in quantum opto-mechanics and quantum sensing.

Benefit for Czechia: CR will gain from the long-term knowledge in this area and mastering new applications coming from this effort among the first in the world.

Quantum networks

Pillars: Quantum Communication, Quantum Simulation, Enabling Science

Contact person: Igor Jex, igor.jex@fjfi.cvut.cz

Institution: Department of Physics, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague

Know how: The group in Prague worked extensively on the properties of quantum networks and their applications to quantum information. We developed a theory to describe the evolution of quantum networks under the influence of perturbations and imperfections. Our theory can be applied to quantum Boltzmann gases, graph-like networks with various degree of complexity. It is capable to give answers to a wide range of problems ranging from transport in random media to possible models of a quantum Internet.

Research goals: We will study the possibilities to model physical systems using quantum networks and focus, among other goals, on their universal properties. This will help to understand the behavior of mesoscopic and macroscopic networks which will find applications in communication protocols of the quantum age.

Excellence, Uniqueness: The members of the group in Prague are respected internationally as experts on quantum networks. Our experience with the theory of iterated quantum maps allows us to tackle a wide range of problems of quantum information and communication applicable in quantum networks.

Benefit for Czechia: Access to the latest research on quantum networks and links to top international groups working in the field.

Quantum walks

Pillars: Quantum Simulation, Enabling Science

Contact person: Igor Jex, igor.jex@fjfi.cvut.cz

Institution: Department of Physics, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague

Know how: Over the past 15 years the group in Prague worked extensively on problems of quantum walks. We studied properties of quantum walks, proposed simple classification schemes and discovered novel types of quantum walks. We have extensive experience with discrete time quantum walk implementations using optical feedback-loops and have been instrumental in realizing the first two-dimensional quantum walk. We work on exploiting quantum walks as instrument to simulate other physical systems and processes like interacting particles or quantum transport.

Research goals: We will study the power of quantum walks as a quantum simulator. In particular we will study the possibilities to mimic transport in complex networks with the aim to find optimal configurations and design proof of principle experiments.

Excellence, Uniqueness: The group in Prague is internationally recognized for its studies of quantum walks and their applications to quantum information processing and quantum simulation. In the framework of the long-standing collaboration with the experimental group of prof. Silberhorn (University of Paderborn, Germany) we participate in implementing theoretical proposals in the state-of-the-art experiments.

Benefit for Czechia: Access to quantum technologies related to quantum walks and collaboration with top international research teams.

Nonlinear optical networks

Pillars: Quantum Simulation, Quantum Computation, Enabling Science

Contact person: Igor Jex, igor.jex@fjfi.cvut.cz

Institution: Department of Physics, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague

Know how: The group in Prague has experience in the analysis, design and fabrication of integrated nonlinear waveguide arrays used as novel types of optical sources of entangled light. We analysed optical waveguide arrays as implementation of quantum walks and designed simple protocols implementing search algorithms. We proposed variants of boson sampling based on nonlinear optical networks offering several advantages in comparison to previous schemes.

Research goals: We will study nonlinear optical networks as possible simulators of quantum dynamics, and as candidates for rudimentary quantum processors that efficiently facilitate algorithms such as boson sampling. We will aim at designing optimal sources of non-classical light with many photons based on waveguide arrays.

Excellence, Uniqueness: The close collaboration with the experimental group of prof. Silberhorn (University of Paderborn, Germany) allows us to propose schemes which put us within reach of experimental realization.

Benefit for Czechia: Access to the latest technology of nonlinear optical networks and links to top international groups working in the field.

Quantum nanophotonics and nanoplasmonics

Pillars: Quantum, Simulation, Quantum Computation, Enabling Science

Contact person: Ivan Richter, ivan.richter@fjfi.cvut.cz

Institution: Department of Physical Electronics, Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague

Know how: Our team has been systematically focused on the studies of theoretical fundamentals of various nanophotonics and nanoplasmonic structures and platforms, such as sub-wavelength structured photonic systems, photonic crystals, meta-materials, plasmonic resonant nanostructures, bio-inspired structures, etc., both in linear and nonlinear optical regimes, in relation to perspective applications. Recently, we have also concentrated on quantum properties of such systems, in connection to nanoscale quantum optics.

Research goals: We will investigate the quantum phenomena in nanophotonic and nanoplasmonics systems as the starting point for developing photonic and plasmonic technologies enabling the quantum-enhanced performances. In particular, we will develop the theoretical techniques capable of predicting and understanding rich quantum phenomena in nanophotonic and nanoplasmonic systems. Also, we will apply these techniques to study such effects as linear and nonlinear light interactions in nanostructured media, using such platforms as plasmonic waveguides, metamaterials, nanoscale resonant structures, graphene plasmonics, etc.

Excellence, Uniqueness: Expertise in theory and simulations of nanophotonic and nanoplasmonic structures and interactions at the nanoscale. Long-term experience in Theoretical exploitation, computer simulations, analysis, and design of photonic and plasmonic structures for applications in nanotechnologies. The group in Prague is known, in the framework of the collaboration, for its studies on the light interactions at the nanoscale and for help in employing theoretical ideas in the realization and experiments.

Benefit for Czechia: Realization of the proposed research will engage the Czech teams in European network working on the perspective research topics. Students involved in these scientific topics will attain the necessary know-how. Access to quantum technologies related to quantum nanophotonics and plasmonic platforms and collaboration with international research teams.

Quantum sensing and imaging using color centers in diamond

Pillars: Quantum Metrology and Sensing, Enabling Science

Contact persons:

- Miloš Nesládek, milos.nesladek@uhasselt.be
- Petr Cígler, petr.cigler@uochb.cas.cz

Institutions:

- Faculty of Biomedical Engineering, Czech Technical University, Kladno
- Institute for Organic Chemistry and Biochemistry, Czech Academy Sciences, Prague

Know how: We have developed luminescent nanodiamond particles with NV or SiV quantum color centers acting as molecular quantum sensors or imagers for molecular events. This includes diamond material as well as complex chemical architecture allowing to construct sensors for specific targets. We have developed photo-electrical readout of the diamond NV spin quantum states in bulk diamond that can be used for ultra-sensitive magnetometry and sensing of electrical fields.

Research goals: Quantum detection of the individual molecules or their structures. Imaging of molecules in biological and chemical environment. Quantum diagnostic methods for image reconstruction. Single-molecular NMR and EPR detection techniques. Theoretical description and quantum sensing protocols. Dynamic nuclear polarization using quantum centers. Detection of electrical and magnetic field, quantum magnetometry by electric readout of quantum states.

Excellence, Uniqueness: Expertise in development of nanodiamond material with controlled content of single NVs, of NV centers ensembles, surface chemical modification and functionalization quantum sensor development. Optical, photo-current and electrical magnetic resonance methods

Benefit for Czechia: Access to modern nanomaterial and diamond fabrication technology and surface modification. Detection technology at quantum level, single molecular quantum diagnostics and imaging. Ultra-sensitive magnetometers for space. Electrical quantum chips.

Self-assembled layers of molecular qubits with tunable spin interactions

Pillars: Quantum Computation, Quantum Simulation, Enabling Science

Contact person: Jan Čechal, cechal@fme.vutbr.cz

Institutions:

- CEITEC, Brno University of Technology, Brno
- Faculty of Science, Masaryk University, Brno
- Faculty of Science, Palacký University, Olomouc

Know how: Synthesis of molecular magnetic and spin-transition compounds and deep knowledge of their properties. Preparation and analysis (structural, optical, functional) of ordered thin films of both inorganic and organic compounds.

Research goals: Development of a highly scalable platform for quantum computation with quantum bits represented by molecular nanomagnets. External control of the interaction between the qubits in the network. Design of novel compounds with required properties and development of approaches to assemble them with sub-molecular precision. Working quantum register of about 10 qubits in the ten-year horizon.

Excellence, Uniqueness: The current research efforts to achieve external control over the spin interaction are unique at international level.

Benefit for Czechia: Realization of the proposed research will involve the Czech teams in European network working on the top-level highly attractive research topics. Students and young researchers actively working on proposed scientific topics will acquire the essential know-how necessary for future commercialization.

Quantum computation and simulation in chemistry

Pillars: Quantum Simulation, Quantum Computation, Enabling Science

Contact persons:

- Jiří Pittner, jiri.pittner@jh-inst.cas.cz
- Libor Veis, libor.veis@jh-inst.cas.cz

Institution: Department of Theoretical Chemistry, J. Heyrovský Institute of Physical Chemistry of the Czech Academy of Sciences, Prague

Know how: We have expertise on development and simulation of quantum algorithms for application in chemistry. We have developed a general code for simulation of a quantum computer on a classical one and used it to implement various quantum approaches (phase estimation, adiabatic state preparation, variational quantum eigensolver) and perform their assessment on realistic chemical models. We have studied problems of non-relativistic molecular Hamiltonians, as well as relativistic or beyond Born-Oppenheimer ones.

Research goals: The main aim is to exploit the advantages of future quantum computers for solving computationally hard problems in chemistry. Nevertheless, we would also like to employ the already available quantum hardware for non-trivial applications.

Excellence, Uniqueness: We have been among the first groups worldwide active in the field of quantum algorithms for chemistry. Recently, we have established a collaboration with a leading group in this direction - prof. Aspuru-Guzik, Harvard University, aimed mainly at development of new variational quantum-classical algorithms suitable for current and near-future quantum computers.

Benefit for Czechia: Establishing the know-how for application of quantum computers in chemistry and collaboration with top international research teams. Once quantum computations become practicable, there will be a huge impact in computational drug and material design.

Quantum information theory and quantum cryptography

Pillars: Quantum Communication, Quantum Computation, Enabling Science

Contact person: Jan Bouda, bouda@fi.muni.cz

Institution: Faculty of Informatics, Masaryk University, Brno

Know how: Multidisciplinary team with background in computer science, mathematics and physics. Shannon's and Renyi information theory, non-iid analysis, randomness analysis.

Research goals: Information theory, efficient generation and usage of randomness, mathematical tools for non-iid analysis, pseudo-random structures, and tools for optimization and concentration of measure. Protocols and cryptographic primitives secure against quantum adversaries. Quantum protocols and primitives achieving quantum-classical separation in security.

Excellence, Uniqueness: Long-term experience in the research in this area, research collaboration with top world and European research teams in this area.

Benefit for Czechia: Development of necessary theoretical background and algorithms for highly secure communication links. Randomness extractors.

Quantum and classical communication complexity

Pillars: Quantum Communication, Quantum Computation, Enabling Science

Contact persons:

- Dmitry Gavinsky, gavinsky@math.cas.cz
- Pavel Pudlák, pudlak@math.cas.cz

Institution: Mathematical Institute of the Czech Academy of Sciences, Prague

Know how: During the last decade we have obtained a number of results demonstrating strong qualitative advantage of quantum communication over classical one. Communication complexity is one of the strongest models of computing where mathematicians can establish hardness of certain computational tasks. Therefore, our separations – some of them are the strongest known today – are among the best theoretical evidences of the advantage that quantum computers can offer.

Research goals: We will continue our investigation of quantum communication, of the quantum query model and of quantum computing in general. The main focus of our research has been and continues to be comparing the abilities of quantum computers to those of classical ones.

Excellence, Uniqueness: Some of our results are the strongest separations between quantum and classical communication complexity known today.

Benefit for Czechia: Understanding advantage of quantum technology over classical computing is crucial. Our research is aimed to give such understanding.

Quantum computing of statistical physics phenomena

Pillars: Quantum Simulation, Quantum Computation, Enabling Science

Contact person: Martin Loeb1, loeb1@kam.mff.cuni.cz

Institution: Department of Applied Mathematics, Faculty of Mathematics and Physics, Charles University, Prague

Know how: Topological quantum computing, enumeration, graph theory, complexity, algorithms, statistical physics.

Research goals: The research will be focused on separating classical and quantum computation and on understanding the advantages of quantum computing for problems coming from statistical physics.

Excellence, Uniqueness: Rigorous understanding of quantum computing of basic statistical physics functions. The attempts towards quantum enumeration form a novel fundamental challenge.

Benefit for Czechia: The cutting-edge quantum technologies are close to what we are doing. Our work connects the Czech environment with the front of quantum technologies. An illustration: There is a possibility to implement practical computations of Ising ground state energy using the D-wave computer at LANL (Los Alamos, U.S.A.). We agreed on further joint work. One of our former students plans a research stay in LANL to test the D-wave computer. Several other members of the Department of Applied Mathematics have expertise in Max-Cut type problems and graph polynomials, which is a relevant expertise for D-wave computation.
