Final research report

Analyzing Quantum Communications in Noisy Environment
OTKA K112125

2015–2018

Introducing the research

Secure communications can be developed by means of quantum channels for data transmission. The security of a quantum channel is based on the no-cloning theorem. The quantum key distribution used to be solved with entangled photon-pairs, but entanglement is highly sensitive to noise, and additionally, the efficiency of single photon detection is usually low. The continuous-variable quantum key distribution (CV QKD) approach gives an opportunity for the transmission of quantum state(s), too. It is proved that the secure key distribution can be demonstrated with CV QKD against arbitrary attacks. Long-distance key distribution can be implemented by a quantum based optical network. Our research group was focusing on extending the possibilities of point-to-point quantum connections and making the first step to constructing a simple quantum network with CV QKD. The results of theoretical research (description of quantum channels) was used in the planning and construction of experimental arrangement.

The aim of the research team was mapping the potential in the future quantum communication networks. We contributed the broadening of the boundaries of information theory horizons by the results obtained during the research. The investigation of quantum key information sharing opens up new opportunities not only in the description of the theoretical modeling and information networks, but also in safe and efficient communication for the society. The relationship between quantum information theory, classical information theory and traditional algorithm theory can be used in the analysis of quantum information theory-based cryptographic protocols.

Furthermore, our team also studied the feasibility of redundancy-free quantum encryption, and the implementation of long distance secure quantum communication too. The group explored issues related to the optimization of the quantum communication networks by high priority. Thanks to the theoretical and practical results of the team, efficient communication may become available in future quantum communication networks in allowing world–wide spread of large–range quantum communication networks

Main focuses of our work

During the four years of the project, we studied the open problems of quantum information and communications, entanglement generation and distribution, quantum cryptographic protocols and quantum computations. The research work was focused on quantum communication networks, quantum key distribution protocols, quantum computers and quantum computer architectures. The research works analyzed the possibilities of entanglement transmission over noisy quantum channels, and entanglement generation between distant points.

The research covered the utilization of quantum computations and algorithms in quantum computers. We analyzed the theory of quantum architectures and quantum computer networks.

In detailed, we worked on the following research problems

Open Problems in the Theory of Quantum Communication including

- Characterization of Quantum Channel Capacities
- Classical and Quantum Capacities of High Dimensional Quantum Channels
- Development of Code Concatenation Techniques for Long-distance Quantum Communications
- Security of Quantum Communications

Open Problems in the Physical Description and Experimental Realization of Quantum Communication including

- Quantum Optics with Single and Few Photon Wave Packets
- Building a repeater for continuous-variable quantum key distribution systems
- Implementation of Continuous Variable Quantum Communication Algorithms

Key results of our research

In the research work, we analyzed the properties of quantum channels, the characterization of quantum channel capacities, the classical and quantum capacities of quantum channels, and defined novel channel structures.

Novel solutions for noisy quantum communications and continuous variable quantum key distribution

In a continuous-variable quantum key distribution (CVQKD) system, the information is conveyed by coherent state carriers. The CVQKD protocols provide a plausible solution to practically realize an unconditional secure communication over standard, currently established telecommunication networks. The amount of tolerable noise and the efficiency of the post-processing steps are crucial points in CVQKD, since it determines the overall performance of the protocol, including the secure key rates and transmission distances. In the research work, we defined advanced solutions to improve the performance of CVQKD protocols. The research proposed novel modulation, transmission and decoding techniques, and post-processing algorithms for CVQKD. The proposed solutions lead to significantly improved transmission efficiency, higher secret key rates, improved tolerable loss, and excess noise. We investigated novel encoding and decoding solutions for CVQKD, and study the role of quantum entanglement in CVQKD systems. The research also investigated the development of encoding and decoding methods for CVQKD-based long-distance quantum communications.

Besides the attractive properties, the CVQKD schemes have an extreme sensitivity to the channel noise and other loss which allow no to use these protocols with such a high efficiency as it is available for traditional protocols in a traditional telecommunication scenario. To resolve the problem of low tolerable loss and excess noise, we introduced a new modulation scheme for CVQKD. The AMQD modulation allows higher tolerable loss and excess noise in comparison with the standard modulation, and can be applied in both one-way and two-way CVQKD. We also investigated an adaptive modulation variance allocation mechanism for the scheme, which can significantly improve the efficiency of the transmission, particularly in the low SNR regimes.

We defined an iterative error-minimizing secret key adapting method for multicarrier CVQKD. A multicarrier CVQKD protocol uses Gaussian subcarrier quantum continuous variables (CVs) for the transmission. The proposed method allows for the parties to reach a given target secret key rate with minimized error rate through the Gaussian sub-channels by a sub-channel adaption procedure. The adaption algorithm iteratively determines the optimal transmit conditions to achieve the target secret key rate and the minimal error rate over the sub-channels. The solution requires no complex calculations or computational tools, allowing for easy implementation for experimental CVQKD scenarios.

We defined the statistical quadrature evolution (QE) method for multicarrier continuous-variable quantum key distribution (CVQKD). A multicarrier CVQKD protocol uses Gaussian subcarrier quantum continuous variables (CVs) for information transmission. The QE scheme utilizes the theory of mathematical statistics and statistical information processing. The QE model is based on the Gaussian quadrature inference (GQI) framework to provide a minimal error estimate of the CV state quadratures.

We proved an equivalence transformation between the correlation measure functions of the causally-unbiased quantum gravity space and the causally-biased standard space. We proposed the Gaussian quadrature inference (GQI) method for multicarrier continuous-variable quantum key distribution (CVQKD). A multicarrier CVQKD protocol utilizes Gaussian subcarrier quantum continuous variables (CV) for information transmission. We demonstrate the results through the adaptive multicarrier quadrature division (AMQD) scheme. Defined direct GQI (DGQI), and proved that it achieves a theoretical minimal magnitude error. Introduced the terms statistical secret key rate and statistical private classical information, which quantities are derived purely by the statistical functions of GQI. Proved the secret key rate formulas for a multiple access multicarrier CVQKD via the AMQD-MQA (multiuser quadrature allocation) scheme. The GQI and DGQI frameworks can be established in an arbitrary CVQKD protocol and measurement setting, and are implementable by standard low-complexity statistical functions, which is particularly convenient for an experimental CVQKD scenario.

Transmission of quantum entanglement will play a crucial role in future networks and long-distance quantum communications. Quantum key distribution, the working mechanism of quantum repeaters and the various quantum communication protocols are all based on quantum entanglement. To share entanglement between distant points, high fidelity quantum channels are needed. In practice, these communication links are noisy, which makes it impossible or extremely difficult and expensive to distribute entanglement. We analyzed the process of entanglement generation over the practical channels, and the exploitation of advanced quantum effects on the enhancement of quantum correlation and entanglement. We introduced advanced solutions for entanglement generation, and for entanglement establishment in quantum communication networks.

New results in quantum optics with T-shaped monolithic grating structures

We worked in detailed examination of T-shaped monolithic grating structures. We worked on how this kind of robust structures with excellent thermo-mechanical properties can be used as dichroic filter, bandfilter or broadband mirror in NIR range of the electromagnetic spectra. For the simulation of structures and for the optimization we applied 4 independent numerical method: FDTD, FDFD, RCWA, MoL. In our 8-page long article we have present all of our results we achieved so far in this topic. We have successfully optimized the geometry of each optical element: dichroic filter, bandfilter or broadband mirror, which hold excellent optical properties as the result of the optimizations. The received results from simulations were always checked by conservation of energy and direct comparison of the results between different methods. The four independent methods used for the simulations have been developed by ourselves in Matlab, hence tuning of the parameters and conditions of stability were fully controlled by us. Nonlinear second harmonic wave generation (SHG) has been thoroughly examined in one dimension both analytically and numerically. Recently, the application of advanced domain poling techniques enabled the fabrication of two-dimensional (2D) patterns of the sign of the nonlinear coefficient in certain nonlinear crystals, such as LiNbO3 and LiTaO3. This method can be used to achieve quasi phase matching in SHG and hence amplification of the second harmonic fields in 2D.

We presented a true vectorial numerical method for the simulation of SHG by extending the finite difference frequency domain method (FDFD). Our nonlinear method (NL-FDFD) operates directly on the electromagnetic fields, uses two meshes for the simulation (for ω and 2ω fields), and handles the nonlinear coupling as an interaction between the two meshes. Final field distributions can be obtained by a small number of iteration steps. NL-FDFD can be applied in arbitrarily structured linear media with an arbitrarily structured χ(2) component both in the small conversion efficiency and the pump depleted cases.

Application of the pseudospectral method in numerical calculations is well established. The method is used in several disciplines, from geology to applied mathematics. The pseudospectral method also appears in computational electromagnetism. Its implementation already has been carried out for the finite element method and finite difference time domain method. We implemented the pseudospectral method for the finite difference frequency domain (FDFD) method, and hence the resulting method is called the pseudospectral frequency domain (PSFD) method. The PSFD method is compared to the FDFD method in terms of the numerical phase velocity and anisotropy. The method is extended for the nonlinear process PSFD (NL-PSFD) of second-harmonic generation. It is shown how a plane wave source at oblique incidence can be implemented, and its performance for tilted quasi-phase-matched grating is discussed. Finally, a specific method is deduced from NL-PSFD for large volume simulation, where only second-order nonlinearity is spatially structured, and a two-dimensional nonlinear photonic crystal is simulated.

Theoretical and experimental noise reducing techniques in quantum communication setup

The research work also analyzed the attributes of the quantum network communications, Internet and the application of QKD protocols in quantum networking and quantum repeaters scenarios. We studied the problem of implementation of CV-QKD based quantum communications in quantum networking scenarios.

When we submitted our research plan in 2014, we have planned to design and build a device which extends the distance between the sender and the receiver: The device could act as a repeater for continuous variable quantum key distribution (CV QKD). When we started our research, our related research goal has slightly changed due to numerous reasons including administration issues with ordering high value equipment at the university, so we were focusing on different noise reducing techniques, since noise is the key in every quantum communication application.

We have successfully reduced the noise in our CV QKD system: one of the main sources is the un-controlled polarization rotation of the pulses traveling from Alice to Bob. For proper operation, at Bob side it is necessary to align the polarization of the pulses to the correct direction. To this end, we have included an automatic polarization controller into our setup at Bob's side. The feedback signal is generated by a home developed low speed photodetector, which measures the field intensity in the reference signal arm of Bob's device, and the polarization controller is programmed to maximize this signal. As a result, the polarization of the incoming pulses is turned in the correct direction.

Publications

We have published our results in numerous journals and international conferences: more than 20 journal articles in referred journals with impact factors (including Q1 and D1 journals, one of them with impact factor 20.23) and more than 20 conference papers. For detailed information, please see the detailed list of publications in the online system at otka-palyazat.hu.

Please note that due to the limitations of the Hungarian Publication Database (MTMT), impact factors of the journal articles are not available for the authors. We provided some of them manually in the online system of otka-palyazat.hu.

Helping students and early carrier investigators

The research group contained experts from the area of quantum computation and communications and from engineering. The leader of the group was Sándor Imre (DSc) from the Department of Networked Systems and Service at BME, senior researcher János Kornis (PhD) and researcher Zsolt Papp (PhD) are the members of Optical Metrology Laboratory at BME. Zsolt Kis (PhD), senior researcher is a member of the Quantum Optics and Quantum Informatics Department at the Wigner Research Center for Physics.

We were able to attract students: Tamás Szarvas, a PhD student who joined the project in 2015 and worked on it until 2018. As young postdoctoral researcher, László Gyöngyösi worked in our project during its four years. Another postdoctoral researcher, László Bacsárdi has joined our research project in 2018. Among others, Győző Gódor (as a young researcher working towards his PhD) joined the research project as well.

Application of the results

The results of our project are not only theoretical, they can be applied in different experimental quantum communications setups as well as can be further utilized by the industry. Based on our research, we were able to join to the national HunQuTech consortium which has 7 members and is working on implementation of quantum technologies. We were able to build new research connections with European researchers under the umbrella of the European Quantum Technology Flagship project (QT) by participating different events of the QT flagship and other meetings.

We are thankful for the OTKA/NKFIH for their support during the four years of the project.

On behalf of the research team,

Sándor Imre
Principal investigator