evropský sociální fond v ČR EVROPSKÁ UNIE MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Název projektu: Mezinárodní centrum pro informaci a neurčitost

Registrační číslo: CZ.1.07/2.3.00/20.0060

Zápis z práce s cílovou skupinou

Název akce: Panelová diskuse, Dr. Laszlo Ruppert (Budapest University of Technology and Economics, Hungary)

Datum: 12. únor 2012

Místo konání: katedra optiky, PřF UP Olomouc

Počet účastníků: 5 akademických a vědeckých pracovníků a 3 studenti

---

Program:
During the scientific discussion the possibilities of state and channel estimation using continuous variables with application to quantum communication were discussed.

Short description of the work wit hhte target group:

- The scientific discussion was dedicated to the possible use of state estimation methods in continuous-variable quantum key distribution. The issue of state and estimation is essential in such task because the trusted parties need to properly estimate the covariance matrix of the two-mode entangled state, shared between them, which is required by the security proofs. Few attempts to reveal the role of estimation in continuous variable quantum key distribution were made recently as the part of finite-size analysis in the groups of prof. Ph. Grangier (France) and prof. R. Werner (Germany). Alternatively, the issue of channel estimation in case of fluctuating channel was addressed in collaboration with the group of prof. G. Leuchs (Germany).

- The participants of the discussion panel agreed that the channel and state estimation must be analyzed taking into account the state profile in the different protocols of quantum key distribution, which are based either on squeezed and coherent states. At the same time the estimation pulses must de indistinguishable from the signal pulses, which is dictated by the security proofs of the protocols.

- The possible further research directions were discussed, which are concerned with the estimation of the covariance matrix elements taking into account the limited number and limited energy of estimation pulses, from which the channel parameters and the subsequent security analysis may be derived. The analysis of the impact of such imperfect estimation on security and optimization of estimation using the proper method of maximum likelihood and unbiased estimators may be the subject of the joint future research.

Příloha č. 1 – prezenční listina

Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.