INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Název projektu: Mezinárodní centrum pro informaci a neurčitost

Registrační číslo: CZ.1.07/2.3.00/20.0060

Zpráva z účasti na stáži

Datum konání stáže:	8.11.2011 – 9.12.2011
Navštívené pracoviště:	CNRS-LPQM, ENS Cachan, Pařiz, Francie
Zahraniční garant:	doc. Frederic Grosshans
Účastník stáže:	Vladyslav Usenko, Ph.D.

Stručný popis navštíveného pracoviště

The Ecole normale supérieure de Cachan (ENS Cachan) founded in 1912 is a prestigious public institution of higher education; it is one of the four major French Grandes Écoles, which are considered as the top higher education institutions in France. The research part of the ENS Cachan consists of 12 laboratories and 2 interdisciplinary research institutes, which makes Cachan a very active research center. Quantum and Molecular Photonics Laboratory (le Laboratoire de photonique quantique et moléculaire, LPQM) is the main physical laboratory in ENS Cachan and is also the part of the CNRS (Centre National de la Recherche Scientifique, National Center for Scientific Research), which is the largest governmental research organization in France and the largest fundamental science agency in Europe. The co-founder of the LPQM laboratory is also France Telecom R&D, which is the research and development division of France Télécom (the main telecommunications company in France, the third-largest in Europe). The directions of research of the LPQM laboratory cover quantum, nonlinear and biological nanophotonics as well as development of components for photonic technologies and studies of hybrid nanostructures. The LPQM staff consists of 15 permanent members (professors, associate professors and post-docs) and over 20 post-graduate students and engineers. The research of the laboratory is supported by several French and European grants (in particular, NanoSci-ERANET "NEDQIT" and IST STREP FP6 "EQUIND").

The theoretical group of Assoc. Prof. F. Grosshans is dealing with the fundamental tests and quantum information and is especially active in quantum cryptography Besides doc. Grosshans it consists of Dr. Fabio Grazioso (post-doc) and Christina Giarmatzi (Ph.D. student). In the tight collaboration with the leading experimentalists in LPQM as well as within CNRS (in particular, group of Prof. Philippe Grangier at CNRS Institut d'Optique), group of doc. Grosshans achieved the outstanding results in the field of quantum information,

e.g., developed the first Gaussian continuous-variable quantum key distribution protocol on the basis of coherent states and shown optimality of Gaussian collective attacks.

Průběh stáže

During the visit the joint research in the field of Gaussian quantum key distribution was performed in collaboration with doc. Grosshans and his colleagues. The vast groundwork performed by the group was actively used for the further development of the field of continuous-variable quantum cryptography. In particular, the methods of security analysis, including entangling cloner and purification methods, based on the covariance matrix calculations, were deeply studied and applied.

The active scientific discussions resulted in the development of the novel Gaussian quantum key distribution protocol, which is based on the linear modulation of the coherent states and subsequent single-quadrature detection. Contrary to the usual symmetric Gaussian protocols, where a coherent state is randomly displaced on the phase-space in two complementary quadratures according to a pair of Gaussian random variables, the linear modulation protocol supposes the displacement in only single quadrature so that the resulting mixture corresponds to the linearly elongated area on a phase space, while the uncertainty of the non-modulated quadrature remains equal to a shot-noise unit. The advantage of such protocol is its relative technical simplicity as it does not require modulation of two quadratures simultaneously so that only amplitude quadrature modulation by means of driving current attenuation can be used, while more complex phase quadrature modulator is not required. Moreover, since the phase quadrature is not modulated, the channel estimation cannot and doesn't have to be performed in the corresponding observable. This technical simplification constitutes also the drawback, because an eavesdropper can apply effective asymmetrical phase-sensitive attacks. Such possibility was, however, cut out by the consideration of the physicality region, limiting the possible eavesdropping attacks. It was shown, that a certain region of parameters exists, when any physically valid attack, provided adequate modulation and channel estimation in one quadrature is performed, is not security breaking even in the worst case assumption. Under such assumption the security bound of the novel protocol were derived in terms of distance and tolerable channel excess noise, which shown that the new asymmetric protocol performs expectedly worse than its symmetric counterpart, but still provides reasonable security region, while enabling essentially simpler technical implementation.

During the visit the laboratory tour was also arranged and the most recent scientific projects currently running at the LPQM laboratory were presented, in particular, in the field of quantum metrology and quantum information processing.

Publikace rozpracované během stáže

The scientific discussions during the stay resulted in the preparation of the manuscript draft with the working title "Continuous variable quantum key distribution with single quadrature modulation" which is currently under preparation to publication and is to be submitted in the first quarter of the year 2012.

Navázání kontaktů

The visit resulted in the establishment of the scientific collaboration with the group of doc. Frederic Grosshans. The new research project was started and the future collaboration will further intensify the scientific contact within the field of continuous-variable quantum information as well as expansion of the research directions. The possible future joint

international projects between the Palacky University and CNRS were also preliminarily discussed.

Shrnutí stáže

The visit indeed achieved its goals, the scientific collaboration with one of the leading European institutions in the field of quantum optics and quantum information was successfully established and intensified. The new knowledge on the current research trends in the mentioned field was obtained and will be further disseminated to the target group within the scientific seminars.

Fotografická dokumentace

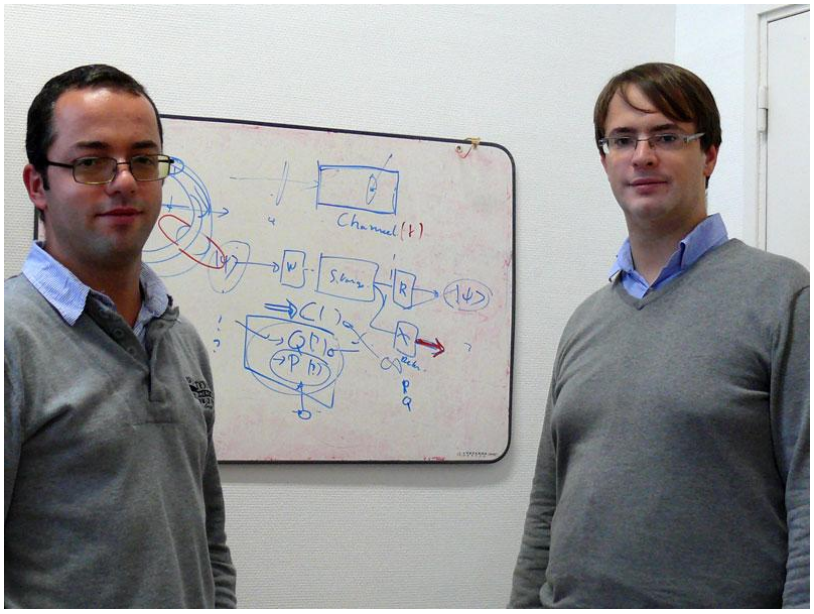

Photo taken during the scientific discussion within the stay, depicted are doc. Grosshans (right) and Dr. Usenko (left).

During the work on the manuscript, doc. Grosshans (right) and Dr. Usenko (left).