ICT10-067 - HiPANQ - High Performance Algorithms for Next Generation Quantum Key Distribution

Abstract

Quantum key distribution (QKD) is a new technology well known for superior long term security of exchanged keys. As such it is an invaluable component to secure future communication infrastructure but its applicability is hampered by its low key rates. A recent break through in single photon detection facilitates the setup of novel high-rate QKD systems which are capable of generating shared keys orders of magnitudes faster than today, if the post-processing can be handled.

QKD post-processing - transforming the correlated and partly secret results of quantum measurements into a secure key - is a computationally intensive task and well elaborated for kbit/s key rates. However, handling higher rates in real-time faces completely new methodological and algorithmic challenges. HiPANQ addresses these and aims at effective methods for QKD rates in the 100 Mbit/s regime. To this end new efficient algorithms for key reconciliation and privacy amplification will be developed.

Keywords:
Quantum Key Distribution, Error Correction, Privacy Amplification, Finite Key Analysis

---

Principal Investigator:	Christoph Pacher
Institution:	AIT Austrian Institute of Technology GmbH
Further collaborators:	Gottfried Lechner (University of South Australia) Renato Renner (ETH Zurich)

Status: Completed (15.11.2010 - 31.12.2013)
GrantID: 10.47379/ICT10067

Further links to the persons involved and to the project can be found under
https://wwtf.at/funding/programmes/ict/ICT10-067/