

Theory and Experimental Research in Quantum Communications

Description

This research line focuses on the development, analysis, and experimental validation of quantum technologies for secure communications. It combines theoretical modeling, protocol design, and security analysis of quantum communication systems - particularly quantum key distribution (QKD) - with experimental implementations and demonstrations. Special emphasis is placed on implementation security, addressing vulnerabilities that may arise in practical realizations of quantum communication protocols.

Research activities include the development of mathematical techniques for the security analysis of real-world implementations, the design and experimental demonstration of fiber-based and free-space quantum communication links, and the investigation of quantum hacking attacks, together with the design and validation of effective countermeasures. The line also explores novel photonic approaches for quantum communications and quantum random number generation inter alia. These efforts aim to advance the security, performance, robustness, and scalability of practical quantum communication systems, while supporting the testing, standardization, and certification of these technologies for their secure deployment in future quantum communication networks.

Infrastructures

For experimental research activities, the fellow will have access to three dedicated laboratories (approximately 90 m² each) equipped with state-of-the-art infrastructure for fiber-based quantum communications, free-space and satellite-based quantum links, as well as facilities for quantum hacking and certification of quantum communication systems. For theoretical research, the fellow will have access to high-performance computing facilities enabling large-scale simulations and advanced modeling of quantum communication protocols.

Keywords

Photonic Quantum Systems | Quantum Communication | Quantum Cryptography | Quantum key Distribution | Quantum Networks | Quantum Technologies