MATTER AND LIGHT FOR QUANTUM COMPUTING

https://ml4q.de

ML4Q Intensive Weeks

Winter Term 2020/2021

Security proofs of quantum key distribution

Lecturer: Dr. Gláucia Murta, Institute for Theoretical Physics III, HHU Düsseldorf

Date: The course is planned for March 2021, more details will come

Course summary:

Quantum key distribution (QKD) is perhaps the most mature of all quantum technologies. Experimental implementations are rapidly developing over the years and, moreover, the security proof of many QKD protocols is very well established.

In this course, we present the concepts and theoretical tools necessary to formalize the security proof and derive the key rates for a quantum key distribution protocol. We will discuss the different adversarial scenarios and the hypotheses present in different security proofs. Finally we will discuss the implications of different hypotheses for experimental implementations of the protocol, reviewing how the failure to match these hypotheses leads to the hacking of quantum cryptosystems.

Universität zu Köln

RWTH AACHEN UNIVERSITY

UNIVERSITÄT BONN

JÜLICH FORSCHUNGSZENTRUM