Quantum Key Distribution Summer School 2026

Sunday, 16 August 2026 - Friday, 21 August 2026

SRS

Program

Abstracts

Christian Schaffner: Information-theoretic security

The term information-theoretic cryptography (ITC) refers to cryptographic methods that are secure even against adversaries with unbounded (quantum) computing power, hence not relying on computational hardness assumptions. This lecture first provides a brief overview of these different types of cryptography and the primitives involved. We introduce mathematical tools such as random variables and Shannon entropy, and present highlights of Shannon's information theory, including the one-time pad encryption scheme and its proof of security via information diagrams. We then cover cryptographic methods and protocols relevant for ITC and QKD, including information-theoretic message authentication, error correction, and privacy amplification. Finally, we briefly discuss computational public-key cryptography, its post-quantum security, and touch upon the question how QKD and post-quantum cryptography can be combined.

Norbert Lütkenhaus: Discrete-variable QKD protocols

We will discuss design principles for good QKD protocols and go through some of the basic QKD protocols. Variations of these protocols will illustrate which aspects are essential, and which are protocol choices. We will also discuss methods of practical evaluation of secret key rates for these protocols.

Renato Renner: Foundations of QKD security

Quantum key distribution has the astonishing property that it allows for information-theoretic security, i.e., we can mathematically prove the security of such protocols even against an all-powerful (quantum) adversary. This lecture delves into the foundations of QKD security, first presenting its definition and the underlying motivation. Building on previously introduced concepts such as privacy amplification, we will line out the essential steps involved in a comprehensive security proof. Furthermore, we discuss the central quantities that have to be evaluated in this context and the techniques employed to accomplish this task.

Peter Brown: Numerical methods for QKD security proofs

Eleni Diamanti: Implementation of QKD protocols

In this lecture, we will discuss practical aspects of optical systems implementing some important QKD protocols. We will go through typical components of such systems, along with criteria and measures for assessing their performance. We will also present examples of configurations and current challenges related to real-life deployment of QKD in fiber optic and satellite networks, integration aspects, and security against side-channel attacks.

Rotem Arnon: Device-independent QKD

In Device-independent QKD (DIQKD) the honest parties, Alice and Bob, do not trust their own devices and, yet, they want to use them to create a shared key. To make such a thing possible, a different type of protocol, based on Bell-inequalities, is required and the security proofs are more demanding. In the lectures, I will explain the basics of DIQKD: The security definition, the fundamental physics that makes DIQKD possible and the main steps of a security proof.

Thomas Jennewein: Space QKD