QuTe
Zentrum für Quantentechnologien

Quantum Information Science Talks

UNIVERSITÄT DES SAARLANDES

Dr. Nico Döttling (CISPA)

(Quantum) Pseudorandom Codes

Error-correcting codes are built to withstand noise, while cryptographic pseudorandomness asks that an object be computationally indistinguishable from a truly random one. Pseudorandom codes (PRCs) aim to reconcile these goals: their codewords remain decodable after noise, yet “look random” to any efficient test. This talk will survey the basic notion and intuition behind PRCs, discuss basic constructions, then focus on what kinds of assumptions are necessary to construct them. We will first provide a black-box impossibility result for PRCs over binary alphabets that decode from a constant fraction of Bernoulli noise: no construction that treats underlying primitives as oracles can succeed relative to a broad class of “local” (noise-sensitive) oracles, including random oracles and trapdoor permutation oracles. We will then turn to the quantum setting: the classical black-box barrier persists even against quantum distinguishers and quantum random oracles, motivating a true quantum analogue. We will introduce quantum pseudorandom codes (QPRCs), where codewords are quantum states indistinguishable from Haar-random, and outline constructions that tolerate noise up to the unique-decoding radius of standard coding schemes.

From https://techcrunch.com/2015/12/18/a-turning-point-for-quantum-computing/

Monday, April 13th, 2026
12:00 PM
Building E2 6, Room E.04

Contact: peter.orth@uni-saarland.de, giovanna.morigi@physik.uni-saarland.de

Website: www.uni-saarland.de/fachrichtung/physik/veranstaltungen/qis-seminar.html