Prof. Dr. Friederike Schmid
Institut für Physik
friederike.schmid@uni-mainz.de

Prof. Dr. Hartmut Wittig
Institut für Kernphysik
hartmut.wittig@uni-mainz.de

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

Physikalisches Kolloquium

Jan. 10, 2023 at 4:15 p.m.
HS KPH

Dr. Nico Döttling
Helmholzt Center for Information Security (CISPA)
in Saarbrücken

Quantum Computing and Cryptography

In the early 1990s cryptography went into a foundational crisis when efficient quantum algorithms were discovered which could break almost all public key encryption schemes known at the time. Since then, an enormous research effort has been invested into basing public key cryptography, and secure computation in general, on problems which are conjectured to be hard even for quantum computers. This research program has been resoundingly successful, leading to unexpected developments, such as the discovery of fully homomorphic encryption schemes. Furthermore, cryptography research has now moved beyond just "post-quantum security", i.e. security against quantum adversaries, and investigates cryptographic protocols for a (still hypothetical) quantum world, where not just adversaries, but also honest users have access to scalable quantum computers and quantum communication channels. This enables applications such as quantum money, which are impossible using purely classical information. In this talk I will give an overview of the field and some of the (in my opinion) most challenging open problems.

Contact:
Daniela Reibel
Sekretariat Prof. Dr. Friederike Schmid
Institut für Physik
reibel@uni-mainz.de

Fulya Mank
Sekretariat Prof. Dr. Hartmut Wittig
Institut für Kernphysik
mank@uni-mainz.de

MATERIALS IN MAINZ SCIENCE

PRISMA+