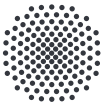

University of Stuttgart
Institute of
Information Security

Hauptseminar: Advanced Topics in Post-Quantum Cryptography

Prof. Dr. Ralf Küsters, Dr. Pascal Reisert

Seminar Announcement

In the upcoming winter term we will offer again a seminar on

Advanced Topics in Post-Quantum Cryptography

Interested students from Mathematics as well as Computer Sciences with a solid background knowledge in algebra (or related fields) are invited to join.

On the Field of Post-Quantum Cryptrography. We heavily rely on cryptography in our everyday life, for example, when we do online shopping and online banking, pay with credit or debit card, open doors with electronic keys, or when we use social networks, instant messengers, online games, WiFi, mobile networks, or electronic currencies.
In all of these applications the most widely used cryptosystems, like RSA encryption and elliptic curve cryptography, are built on the hardness of certain algebraic problems, like the factorization of integers. While these problems withstood all attacks by classical computers so far, it is also known that a suitable quantum computer could easily solve the underlying mathematical problems in polynomial time and therewith break the corresponding cryptosystems. For example, the famous quantum algorithm by Shor can break the factorization problem efficiently.
Recent progress in the development of quantum computers led researchers and governmental organizations, e.g. the National Institute of Standards and Technology (NIST), to start the search for new cryptosystems usable on classical computers that can withstand attacks by quantum computers - so-called post-quantum cryptosystems. Although there are currently no sufficiently powerful quantum computers, it is still highly necessary to find and establish these post-quantum cryptographic standards in due time. This is particularly important for information which has to be kept secret for 5 or 10 years or even longer and which should not become public the moment someone constructs a powerful quantum computer.

The seminar addresses both mathematics behind modern post-quantum secure cryptographic primitives, e.g. algebraic number theory, the cryptographic tools themselves, e.g. post-quantum secure cryptosystems or commitment schemes, and possible applications like Multi-Party Computation (MPC).

Questions? Feel free to contact us by e-mail to
pascal.reisert@sec.uni-stuttgart.de.

SEC