RUB Faculty of Computer Science
www.informatik.rub.de

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

RUB

Theory Colloquium

Friday | July 29 | 12:00
Room GD 03/150

Prof. Dr. Vipul Goyal

Fast Communication Efficient Secure Multi-Party Computation

Secure Multi-Party Computation (MPC) is a framework where multiple parties collaborate to compute a common function of their interest without revealing their private inputs to each other. MPC is a very general cryptographic tool and is useful in diverse situations such as privacy preserving machine learning, secure auctions, and voting. While the feasibility of MPC has been known for several decades, the key challenge is making these protocols efficient.

In this talk, I will describe some of our recent work in making MPC more communication efficient. We focus on the so called information theoretic setting where security doesn‘t rely on unproven cryptographic assumptions (such as factoring). Instead we assume that a constant fraction of the parties behave honestly. This is natural in settings such as Blockchains or voting. We will rely on a tool called packed secret sharing which allows one to run the circuit computation faster by handling a „batch of gates“ at a time instead of a single gate.

Organizers: Michael Walter (RUB) and Giulio Malavolta (MPI-SP)