Bernoullis Tafelrunde

Graduate Student Seminar

Wednesday, 23 November, 13:15-14:00
Seminarraum 05.002, Spiegelgasse 5

Türkü Özlüm Çelik

IRMAR, Université de Rennes 1

Arithmetic via Hyperelliptic Curves

Abstract

In the first part of the talk, we will look at the group structure on hyperelliptic curves and a way how to implement it. After that we will look at the construction of the Kummer surface associated to a hyperelliptic curve. Even though the Kummer surface does not come with a group law, we will consider a pseudo-group structure on it which allows us to define a 'scalar multiplication' that underlies some cryptographical applications.