Bernoullis Tafelrunde

Graduate Student Seminar

Friday, 31 March 2017, 14:15-15:00
Seminarraum 05.001, Spiegelgasse 5

Marius Vuille

EPFL

Towards hyperelliptic curve cryptography

Abstract

Nowadays communication strongly relies on the use of efficient and secure cryptosystems. In this talk, I will present the idea of public key cryptography, together with its most commonly used cryptosystems such as RSA, Diffie-Hellman and El Gamal. In a second part I will explain the role of elliptic curves for establishing the discrete logarithm problem (DLP), and then its natural generalisation to higher genus curves, which leads to my research topic, the efficient computation of isogenies in genus 3.