BRUSSELS SUMMER SCHOOL OF MATHEMATICS
September 3-7,2018

Multilinear maps in cryptography

July 28, 2018

Luca Notarnicola

Abstract

Recently, multilinear maps have received a lot of attention in cryptography. Roughly speaking such maps are generalizations of pairings, i.e. bilinear non-degenerate maps $G_1 \times G_2 \to G_3$ for groups G_1, G_2, G_3 that satisfy some cryptographic security conditions. It is especially interesting to look at pairings on elliptic curves, which have allowed Antoine Joux, in 2000, to describe a first secure key exchange between 3 people.

In this talk we will first define multilinear maps and introduce some basic arithmetic of elliptic curves in order to understand the key exchange protocol on elliptic curves by Joux. To conclude, we will show how multilinear maps allow to generalize this key exchange protocol to a communication protocol between more than 3 people.