Elliptic Curves Cryptography and Lenstra’s Method

Angelo Iadarola

19 May 2016 09:30, Room 1BC45

Abstract

The aim of this talk is to present some important applications of elliptic curves in the world of cryptography. First of all I will recall the main results about elliptic curves which will be useful for the applications, such as Weierstrass form, Group Law and Hasse Theorem, just to put everyone up to par. Then I will shift to the first application, which is the ElGamal cryptosystem on elliptic curves, a public key method related to the Dlog problem for elliptic curves, and its use for the problem of the Digital Signature. Finally I will present an overview of one of the main applications of elliptic curves to cryptography, namely the Elliptic Curves Factorization Method, a probabilistic algorithm for factorization presented for the first time by Hendrik Lenstra in 1987, and up to now still one of the most used. Since 1987 the method has been slightly improved, but I will abide by the first version.

Furthermore, during the talk, in order to give consistency to my arguments, I will cite some other algorithms, but in those cases I will just give the computational complexity, which is the important fact for my aim, and I will introduce some more technical tools.

References
