Groebner bases and ECDLP: involution

Michela Ceria

Abstract: In a recent paper, Amadori, Pintore and Sala proposed a multivariate approach to the study of discrete logarithm problem for elliptic curves, using Semaev's summation polynomials and reducing the computation to only one Groebner basis. The classical Groebner theory is now obsolete and the winning approach by Faugère is strongly depending from a precise implementation. In this talk we will deal on how to compute the aforementioned basis by means of the theory of involution, giving an alternative approach.