EDLYN TESKE, University of Waterloo

Solving the ECDLP using Semaev Polynomials, Weil Descent, and Groebner basis methods – an experimental study

At EUROCRYPT 2012, Petit and Quisquater suggested that there may be a subexponential time algorithm for the Elliptic Curve Discrete Logarithm Problem (ECDLP) in characteristic two fields. This algorithm uses Semaev polynomials and Weil Descent to create a system of polynomial equations that subsequently is to be solved. Its analysis is based on unproven heuristic assumptions on the performance of Groebner basis methods in this particular setting. While the subexponential behaviour would manifest itself only far beyond the cryptographically interesting range, this result, if correct, would still be extremely remarkable. We examined some aspects of the Petit-Quisquater assumptions experimentally. This is joint work with Michael Shantz.