The Schoof-Elkies-Atkin algorithm in characteristic 2

Frederik Vercauteren
Katholiek Universiteit Leuven
K. Mercierlaan 94
B-30001 Heverlee
Belgium
+32 16 32 11 34
Email: Frederik.Vercauteren@esat.kuleuven.ac.be

30 April 2000

Keywords: Elliptic Curves, SEA-algorithm.

The best known general attacks on elliptic curve cryptosystems have running time proportional to the square root of the largest prime factor dividing the group order. Therefore it is necessary to explicitly determine the number of rational points whilst generating secure elliptic curves.

The Schoof-Elkies-Atkin algorithm is the most efficient algorithm to determine the group order of elliptic curves over finite fields. We will present a number of optimizations specific for the characteristic two case. With our implementation, we were able to count the number of rational points on a curve defined over $\mathbb{F}_{2^{1999}}$, which is the current world record for the characteristic two case. The total time needed on one Pentium II 400 MHz would have been about 65 days. The previous record by Reynald Lercier determined the number of points on an elliptic curve defined over $\mathbb{F}_{2^{1663}}$.

Furthermore we will present accurate statistics in the range of interest to cryptography, i.e., for elliptic curves defined over $\mathbb{F}_{2^n}$, with $163 \leq n \leq 431$. With our implementation we can count the number of points on a random elliptic curve over $\mathbb{F}_{2^{163}}$ in less than 10 seconds on a Pentium III 600 MHz.