Elliptic Curves in Cryptography

Ian Blake, Gadiel Seroussi and Nigel Smart

Updates (As of August 29, 2000)

p. 26: Line 2. The suspicions are explained in the paper of S.D. Galbraith and N.P. Smart (*A cryptographic application of Weil descent, Proc. IMA Cryptography and Coding, Springer LNCS 1746, pp 191-200,1999).*

These ideas were further expanded in a paper of Gaudry, Hess and Smart (*Constructive and Destructive Facets of Weil Descent on Elliptic Curves*, Preprint 2000).

Section IV.2: Mention should be made of the recent paper of L. O'Connor (*An analysis of exponentiation based on formal languages.*, EUROCRYPT '99, LNCS 1592, 375–388, 1999). This gives a nice method to determine expected running times for various exponentiation techniques. The method presented also allows the determination of the higher moments, and hence the variance of the running time.

Section VI.5: Reference should be made here to a recent paper of S.D. Galbraith and J. McKee (*The probability that the number of points on an elliptic curve over a finite field is prime*, Preprint, 1999).

Chapter VII: There is a new method of T. Satoh (*The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, Preprint, 1999), which gives an algorithm for point counting on elliptic curves over $\mathbb{F}_{p^n}$ which runs in time $O(n^{3+\epsilon})$, where the O-constant depends, badly, on p.

Work of M. Fouquet, P. Gaudry, R. Harley has extended this to the case of characteristic two, and currently the world record for point counting is for a curve over a field of 2^{5003} elements.

Section X.3: There is a new hyperelliptic discrete logarithm algorithm by P. Gaudry (*An algorithm for solving the discrete log problem on hyperelliptic curves*, in Eurocrypt 2000, Springer-Verlag LNCS 1807, 19-34 2000). This paper gives a very fast algorithm in practice for certain hyperelliptic curves of genus, roughly, four and above.