The Elliptic Curve Discrete Logarithm Problem: State of the Art

Alfred Menezes

Department of Combinatorics & Optimization
University of Waterloo
ajmeneze@uwaterloo.ca

Abstract. Elliptic curve cryptography was invented by Neal Koblitz and Victor Miller in 1985. However, for many years its security was viewed with suspicion by cryptographers. These fears were not entirely meritless, especially in light of the subsequent (and ongoing) development of innovative algorithms for solving special instances of the elliptic curve discrete logarithm problem (ECDLP) and the discrete logarithm problem in the divisor class groups of other families of algebraic curves. Surprisingly, cryptographers seem to have cast aside their fears after the invention of pairing-based cryptography in 2000. I will overview progress made on algorithms for solving the ECDLP and related problems, and will examine the long and curious struggle for ECC acceptance.