Abstract

In 1989, Koblitz proposed using the jacobian of a hyperelliptic curve defined over a finite field to implement discrete logarithm cryptographic protocols. This paper provides an overview of algorithms for performing the group law (which are necessary for the efficient implementation of the protocols), and algorithms for solving the hyperelliptic curve discrete logarithm problem (whose intractability is essential for the security of the protocols). Also considered are destructive applications of hyperelliptic curves — solving instances of the elliptic curve discrete logarithm by using the technique of Weil descent to reduce them to instances of the hyperelliptic curve discrete logarithm problem.