Abstract

This paper aims at introducing generalized Jacobians as a new candidate for discrete logarithm (DL) based cryptography. The motivation for this work came from the observation that several practical DL-based cryptosystems, such as ElGamal, the Elliptic and Hyperelliptic Curve Cryptosystems, XTR, LUC as well as CEILIDH can all naturally be reinterpreted in terms of generalized Jacobians. However, usual Jacobians and algebraic tori are thus far the only generalized Jacobians implicitly utilized in cryptography. In order to go one step further, we here study the simplest nontrivial generalized Jacobians of an elliptic curve.

In this first of a series of articles, we obtain explicit formul allowing to efficiently perform arithmetic operations in these groups. This work is part of our doctoral dissertation, where security aspects are considered in depth. As a result, these groups thus provide the first concrete example of semi-abelian varieties suitable for DL-based cryptography.