

The aim of the thesis is to describe and implement the elliptic curve factorization method using curves in Edwards form. The thesis can be notionally divided into two parts. The first part deals with the theory of Edwards curves especially with properties of elliptic function fields. The second part deals with the factorization algorithm using Edwards form both formally and practically in the way the algorithm is really implemented. The contribution of this thesis is the enclosed implementation of the elliptic curve factorisation algorithm which can be run on a graphic card and which is faster than the state-of-the-art implementation GMP-ECM.