Elliptic-Curves-Based Algoritms in Cryptography

Nicolae CONSTANTINESCU
Faculty of Mathematic and Informatics
University or Craiova
Romania
e-mail: nikyc@central.ucv.ro

Abstract

Let be an elliptic curve *E.* Starting from its definition it is created a set of restrictions which helps to realize an implementation in a real system of the theories concerning the infeasibility of the ECDL problem. There are also presented the implementation methods for the computation of fhe necessary parameters in such a system.

AMS Classification: 94A60, 68P25.

Key words: Criptography, Data encryption.