Edwards model of elliptic curves defined over any fields

Oumar Diao[1] and Emmanuel Fouotsa[2]

[1]Université de Rennes I, Laboratoire IRMAR, Campus de Beaulieu, 35042 Rennes Cedex, France, oumar.diao@univ-rennes1.fr
[2]Département de Mathématiques, Université de Yaoundé 1, Yaoundé Cameroun, emmanuelfouotsa@prmais.org

July 13, 2012

Abstract

In this paper, we present an Edwards model for elliptic curve which is defined over any field and in particular for field of characteristic 2. This Edwards model extends the well known Edwards model over fields of characteristic zero and is ordinary over binary fields. For this, we use theta functions of level four to obtain an intermediate model that we call a level 4-theta model. This model enable us to obtain our new Edwards model with a complete and unified group law. Over binary fields we have a very efficient arithmetic on ordinary elliptic curve.
Keywords: Edwards model, elliptic curve, efficient arithmetic, complete addition law, theta functions, Riemann relations.