Implementación de suma y doblado de un punto en una curva de Edwards en un campo binario

Implementation of addition and doubled of a point on a curve in a field Edwards binary

Fabián Velasquez[1], Javier Vargas[2], Sebastián Puente[3]

[1]M.Sc. Matemática Aplicada, [2]M.Sc. Administración Educativa, [3]M.Sc. Ciencias de la Información y las Comunicaciones
[1, 2, 3] Facultad de Ciencias Básicas e Ingeniería, Grupo de Investigación Macrypt, Universidad de los Llanos. Villavicencio, Colombia. Email: fvelasquez@unillanos.edu.co

Recibido 19/04/2016
Aceptado 11/04/2017

Cite this article as: F. Velasquez, J. Vargas, S. Puente, "Implementation of addition and doubled of a point on a curve in a field Edwards binary", Prospectiva, Vol 15, N° 2, 33-39, 2017.

RESUMEN

En este artículo se presentan los resultados del diseño y desarrollo de operaciones de la aritmética de curvas de Edwards en el campo de Galois GF (2251). Se implementaron las operaciones de suma y doblado de puntos en una curva de Edwards binaria basado en la aritmética de campo finito utilizando una base polinomial. La evaluación de las operaciones se realizó sobre un sistema multiprocesador MPSoC, utilizando las capacidades de multiprocesamiento. En las operaciones de la aritmética en curvas de Edward y campos finitos se utilizan algoritmos eficientes y adecuados para un sistema de multiprocesamiento MPSoC Propeller.

Palabras clave: MPSoC; Propeller; Aritmética de curvas de Edwards; Aritmética de campos finitos, Curva binaria de Edwards.

ABSTRACT

This article presents the results of the design and development of operations of arithmetic of curves of Edwards in the field of Galois GF (2251). Is implemented the operations of sum and bent of points in a curve of Edwards binary based on the arithmetic of field finite using a base polynomial. The operations were evaluated on a system multiprocessor MPSoC, using multiprocessing capabilities. Operations of arithmetic in finite fields and Edward curves are used in appropriate and efficient algorithms for a multiprocessing system MPSoC Propeller.

Key words: MPSoC; Propeller; Edwards curve arithmetic; Arithmetic of finite fields; Binary Edwards curve.

Doi: http://dx.doi.org/10.15665/rp.v15i2.716