International J. of Multidispl.Research & Advcs. in Engg.(IJMRAE),
ISSN 0975-7074, Vol. 5, No. III (July 2013), pp. 85-93

REALIZATION OF FPCA IN SCALAR MULTIPLICAITON ALGORITHMS FOR FPGA IMPLEMENTATION

S. DEIVASIGAMANI
Lecturer, Faculty of Engineering and Computer Technology
AIMST University, Malaysia

Abstract

The present paper describes the methodology and design of fast adder. Also imbibe to deal with carry save arithmetic adders. The fast adder circuits with fast elliptic curve scalar multiplication explore in selective use of carry-save arithmetic. It can accelerate through a variety of arithmetic dominated circuits. Carry plays a major role in all cryptography algorithms such as multiplication and addition. In scalar multiplication addition and doubling engage with repetition. To address this concern the paper also introduces the concept field programmable counter array use with generalized parallel counter. Designed counter reduces the area and compare with the expecting result with some fundamental adders.

Keywords : Carry-save arithmetic, ECC doubling algorithm, Field-programmable counter array (FPCA)**,** Generalized parallel counter (GPC), Scalar Multiplication.