HIGH- PERFORMANCE ARCHITECTURE FOR ELLIPTIC CURVE CRYPTOGRAPHY OVER BINARY FIELD USING HYBRID AND BOOTH MULTIPLIERS

M.K.Ganeshkumar
Computer science & Engineering
Mohamed Sathak Engineering College
Kilakarai,India
itganeshkumar@gmail.com

S.Ramamoorthi
Computer Science & Engineering
Mohamed Sathak Engineering College
Kilakarai,India
ramamoorthis@gmail.com

Abstract—This paper presents a high-performance Elliptic Curve Cryptography(ECC)architecture over binary field, using hybrid and booth multipliers based on the Montgomery scalar multiplication algorithm to perform Point Addition and Point Doubling.ECC provide the secure communication among portable device with small key length. Scalar multiplication is the key operation on the ECC,scalar multiplication on the ECC is Time, Power and Area expensive. The proposed ECC architecture over binary field is designed with three different multipliers namely Array, Hybrid low power encoded multipliers and modified booth multipliers. These multipliers are used in the The word-serial finite field arithmetic unit (AU)is proposed with the optimized operation scheduling and bit-parallel modular reduction.With adedicated squarer,the 160-bit point scalar multiplication with coordinate conversion can be done in575μs,511$\mu s$by the design of one AU,and can be further improved to373μsbytheoneofthreeAUs, both using frequency 100MHZ and 19176,16260 and 8743 LUTs in array, modified booth multiplier and hybrid multipliers respectively.The comparison with other ECC designs justifies the effectiveness of the proposed architecture in terms of performance and area-time efficiency.The architecture is implemented using Spartan3E family device XC3S1600E using Model sim 5.7 and Xilinx 9.2i.

Index Terms-Montgomery Multiplication algorithm, Galois fields, Elliptic curve cryptography, point doubling, point addition, public-key cryptography,hrbrid low power encoded multiplier, array multiplier, modified booth multiplier