Remodeling of Elliptic Curve Cryptography Scalar Multiplication Architecture using Parallel Jacobian Coordinate System

Adnan Abdul-Aziz Gutub  
aagutub@uqu.edu.sa  
Center of Excellence in Hajj and Omrah Research, Umm Al-Qura University  
P.O. Box: 6287, Makkah 21955, Saudi Arabia

Abstract

In this paper, an improved parallel elliptic curve processor is designed and modeled. We adjusted the Jacobian coordinates system by interacting point double and point add operations. This modified coordinates is parallelized using four multipliers similar to older parallel architectures. We implemented the components of the proposed design using FPGA with parametric features, in terms of number of parallel multipliers, number of parallel adders and width of input operands. The remodeled design is compared to other similar designs i.e. parallel Jacobian coordinates and parallel standard projective coordinates yielding better performance. Results showed that this proposed modified Jacobian design gave higher speed and cost (AT^2) showing attractive research direction.

Keywords: Cryptography hardware, Elliptic curve cryptography; Jacobian coordinate system; Parallel multipliers architecture; Projective coordinate cryptosystems

Publisher: CSC Journals, Kuala Lumpur, Malaysia