Preference of Efficient Architectures for GF(p) Elliptic Curve Crypto Operations using Multiple Parallel Multipliers

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

Abstract

This paper explores architecture possibilities to utilize more than one multiplier to speedup the computation of GF(p) elliptic curve crypto systems. The architectures considers projective coordinates to reduce the GF(p) inversion complexity through additional multiplication operations. The study compares the standard projective coordinates (X/Z, Y/Z) with the Jacobian coordinates (X/Z^2, Y/Z^3) exploiting their multiplication operations parallelism. We assume using 2, 3, 4, and 5 parallel multipliers and accordingly choose the appropriate projective coordinate efficiently. The study proved that the Jacobian coordinates (X/Z^2, Y/Z^3) is preferred when single or two multipliers are used. Whenever 3 or 4 multipliers are available, the standard projective coordinates (X/Z, Y/Z) are favored. We found that designs with 5 multipliers have no benefit over the 4 multipliers because of the data dependency. These architectures study are particularly attractive for elliptic curve cryptosystems when hardware area optimization is the key concern.

Keywords: Modulo multipliers, Elliptic curve cryptography, Jacobian projective coordinates, Parallel multipliers crypto hardware.

Publisher: CSC Journals, Kuala Lumpur, Malaysia