On the design of projective binary Edwards elliptic curves over GF (p) benefitting from mapping elliptic curves computation to variable degree of parallel design

ABSTRACT

Finding multiplicative inverse (Modular Inversion) operation is the most time-consuming operation in Elliptic Curve Crypto-system (ECC) operations which affects the performance of ECC. Moreover, several factors that affect the design of ECC have not been intensively investigated in the majority of researches related to ECC, Such as system utilization, area, resources-consuming and area*time cost factors, which play significant role in designing efficient ECC for different applications. This work applies Binary Edwards ECC point doubling operation over GF(p) using projective coordinates instead of affine coordinates due to its ability to remove the long time inversion operation by converting it to a number of multiplication operations. We also utilize the inherent parallelism in ECC operations by mapping its computations to parallel hardware design, in order to improve the performance of ECC. Our results show that the shortest time delay is achieved using 7-Parallel Multipliers (PM) design with projection (X/Z, Y/Z), which overcomes both serial design and the design with affine coordinates. Furthermore, this research proposes a variety of design choices by varying the degree of parallelism to tune-up several factors that affect ECC in order to investigate possible enhancements. It is shown by our experiments that the hardware utilization can be improved by 55%, with less area, and acceptable timeconsuming level compared to other designs in the same projection. In other words, we compromise th performance to enhance system utilization degree, and AT cost, and to reduce area and resourceconsuming. This trade-off between factors is useful to determine the efficient design to be used for different ECC applications based on their requirements and available resources. Especially, when the time-consuming is not the main priority.

Keyword: Elliptic Curves Crypto-system; Point doubling operation; Projective coordinates systems; Parallel design; Hardware utilization; Time-consuming; Area