Hardware architectures & designs for projective elliptic curves point addition operation using variable levels of parallelism

ABSTRACT

Although ECC protocol is considered one of the most secure schemes for information security; it also suffers in its arithmetic computations from the modular inversion operation which is known to be time consuming operation. In the addition operation, Many ECC designs that use projective coordinates over GF (p) have not considered a balance between area, hardware utilization, and performance factors which is important in many ECC applications. In this research we proposed to use the projective coordinates systems to compute the ECC point addition operation with no inversion operations due to the ability to convert each inversion to several multiplication operations that can be applied in parallel. We also present several architectures and design choices for point addition operation that will help to build ECC Coprocessor. These architectures consider different levels of parallelism which may give different choices in ECC design in terms of time and space. This paper proposes the different hardware architectures to design ECC Processor by varying the degree of parallelization benefiting from the inherent parallelism for ECC addition operation. It was shown that the throughput of the design with 4 parallel multipliers enhanced the system performance by 400% and 340% for both projections (X/Z, Y/Z), and (X/Z2, Y/Z3) respectively while the design with 5 parallel multipliers is considered the best fit for projection (X/Z, Y/Z2) due its ability to best utilize and parallelize the hardware arithmetic operations. However, the projection (X/Z, Y/Z) when applied using 4 parallel multipliers gave the best results in terms of hardware utilization, parallelization enhancements and cost factor which make it the first choice when you design the ECC Coprocessor using projective coordinates. A trade-off between security, area and performance is which control the ECC Coprocessor design, the more parallelization you make the more area needed the less time required which will lead to a better performance.

Keyword: Elliptic curves cryptography; Point addition; Projective coordinates